Suvi Laitinen

Älypuhelinten biometriset tunnistus-menetelmät ja niiden tietoturva

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintätekniikka

Insinöörityö

25.4.2025

Tiivistelmä

Tekijä:	Suvi Laitinen
Otsikko:	Älypuhelinten biometriset tunnistusmenetelmät ja niiden tietoturva
Sivumäärä:	41 sivua
Aika:	25.4.2025
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikka
Ammatillinen pääaine:	Mobile Solutions
Ohjaajat:	Yliopettaja Antti Piironen

Insinöörityössä tarkasteltiin älypuhelimissa käytettäviä biometrisiä tunnistusmenetelmiä, kuten sormenjälkitunnistusta, kasvojentunnistusta ja iiristunnistusta. Työn tavoitteena oli perehtyä menetelmien toimintaperiaatteisiin, luotettavuuteen ja tietoturvaan sekä pohtia tulevaisuuden kehityssuuntia ja eettisiä ongelmakohtia.

Työ toteutettiin kirjallisuuskatsauksena, jossa perehdyttiin nykyisiin tunnistusteknologioihin sekä niiden toiminnan vertailuun eri arviointikriteereiden perusteella. Lisäksi perehdyttiin eri hyökkäystapoihin ja haavoittuvuuksiin, joille biometriset tunnistusjärjestelmät voivat altistua. Tulevaisuuden teknologioita, kuten käytöksellisiä biometrisiä menetelmiä ja tekoälyn soveltamista, käsiteltiin mahdollisuuksien ja haasteiden näkökulmasta. Työssä tarkasteltiin myös eettisiä kysymyksiä, kuten käyttäjien suostumusta ja syrjintäriskejä.

Tuloksista ilmeni, että biometriset tunnistusmenetelmät voivat tarjota käyttäjille helppokäyttöisen ja yksilöllisen tavan suojata henkilökohtaisia tietoja, mutta ne eivät ole täysin suojassa väärinkäytöksiltä tai hyökkäyksiltä. Biometristen tietojen suojaus ja läpinäkyvyyden puuttuminen osoittautui keskeiseksi tietoturvahaasteeksi.

Avainsanat: biometrinen tunnistautuminen, sormenjälki, kasvojentunnistus, tietoturva

---

Tämän opinnäytetyön alkuperä on tarkastettu Turnitin Originality Check -ohjelmalla.

Abstract

Author:	Suvi Laitinen
Title:	Biometric authentication methods in smartphones and their security
Number of Pages:	41 pages
Date:	25 April 2025
Degree:	Bachelor of Engineering
Degree Programme:	Information and Communication Technology
Professional Major:	Mobile Solutions
Supervisors:	Antti Piironen, Principal Lecturer

This study examined biometric authentication methods used in smartphones, such as fingerprint recognition, facial recognition and iris recognition. The objective was to explore the operating principles, reliability and security of these methods, as well as to consider future development directions and ethical challenges.

The study was conducted as a literature review, focusing on current authentication technologies and comparing their functionality based on various evaluation criteria. In addition, the research delved into different types of attacks and vulnerabilities that biometric authentication systems may encounter. Future technologies, such as behavioural biometrics and the application of artificial intelligence, were discussed from both the perspective of potential and challenges. Ethical issues, such as user consent and the risk of discrimination, were also examined.

The results indicated that biometric authentication methods can provide users with a convenient and personalized way to protect personal data, but they are not fully protected against misuse or attacks. The protection of biometric data and the lack of transparency emerged as key information security challenges.

Keywords: biometric authentication, fingerprint, facial recognition, security

Sisällys

Lyhenteet

2FA: *Two-Factor Authentication*. Kaksivaiheinen tunnistautuminen, joka edellyttää kaksi erilaista teknologiaa käyttäjän tunnistamiseksi, esimerkiksi salasanan ja sormenjäljen.

CR: *Challenge-Response*. Protokolla, jossa käyttäjälle asetetaan haasteita osana tunnistautumisprosessia.

EER: *Equal Error Rate*. Biometrisessä tunnistuksessa käytettävä mittari, joka kertoo FAR- ja FRR-arvojen risteyskohdan. Tässä kohdassa arvot ovat samat.

EKG: *Elektrokardiogrammi*. Sydämen sähköimpulsseja kuvaava käyrä.

FAR: *False Acceptance Rate*. Biometrisessä tunnistuksessa käytetty mittari, joka kertoo, kuinka usein järjestelmä hyväksyy väärän henkilön oikeaksi käyttäjäksi.

FRR: *False Rejection Rate*. Biometrisessä tunnistuksessa käytettävä mittari, joka kertoo, kuinka usein järjestelmä hylkää oikean käyttäjän tunnistautumisen.

MFA: *Multi-Factor Authentication*. Monivaiheinen tunnistautuminen, joka edellyttää kolme erilaista teknologiaa käyttäjän tunnistamiseksi, esimerkiksi salasanan, sormenjäljen ja kertakäyttöisen koodin.

PCR: *Palm Contact Response*. Tunnistautumisjärjestelmä, jossa käyttäjän kämmenen kosketus vastaa ultraäänisignaaliin ja sen heijastuksiin.

TAM: *Technology Acceptance Model*. Teknologian omaksumismalli, joka kuvaa, miten käyttäjät suhtautuvat uuteen teknologiaan.

TEE: *Trusted Execution Environment*. Suojattu ympäristö laitteen sisällä, joka eristää arkaluontoiset tiedot muusta järjestelmästä ja tarjoaa suojan luvattomalta pääsyltä suojattuun dataan.

XAI: *Explainable Artificial Intelligence*. Selittävä tekoäly, joka pyrkii tekemään tekoälyn päätöksenteon ymmärrettäväksi ja läpinäkyväksi.

1 Johdanto

Matkapuhelimet ovat kehittyneet yksinkertaisesta laitteesta monikäyttöisiksi älylaitteiksi, joita käytetään päivittäin muun muassa maksutapahtumiin, tunnistautumiseen ja henkilökohtaisten tietojen säilyttämiseen. Samalla, kun älypuhelimen rooli on kasvanut, myös tietoturvan merkitys on korostunut. Biometriset tunnistusmenetelmät, kuten sormenjälki- ja kasvojentunnistus ovat nousseet keskeiseen asemaan älypuhelinten turvallisuudessa ja käytettävyydessä. Niiden tavoitteena on tarjota käyttäjille helppo ja yksilöllinen tapa suojata laitteensa ja henkilökohtaiset tietonsa ilman kirjoitettavia salasanoja tai PIN-koodeja.

Vaikka biometrinen tunnistus koetaan usein turvallisemmaksi kuin perinteiset salasanat, menetelmiin liittyy monia tietoturvahaasteita, jotka voivat vaarantaa käyttäjän yksityisyyden ja henkilökohtaiset tiedot. Esimerkiksi biometrisen datan väärinkäyttö, tietomurrot ja järjestelmien haavoittuvuudet voivat altistaa käyttäjät identiteettivarkauksille ja muille tietoturvauhille. Toisin kuin salasanan, biometrisen piirteen, kuten sormenjäljen tai kasvojen, vaihtaminen ei ole mahdollista, mikä tekee datan suojaamisesta erityisen tärkeää. Suojaamisen tärkeys herättää kysymyksiä siitä, kuinka turvallisia nämä menetelmät todella ovat ja missä määrin käyttäjät ovat valmiita hyväksymään tietoturvariskit mukavuuden nimissä.

Biometristen tunnistusmenetelmien jatkuva kehitys on parantanut niiden tarkkuutta ja tuonut markkinoille uusia innovatiivisia menetelmiä. Samalla kasvaa tarve arvioida sekä uusien että vanhojen teknologioiden eettisiä vaikutuksia ja käytettävyyttä eri käyttäjäryhmille. Biometristen tunnistusmenetelmien luotettavuus herättää kysymyksiä niiden yhdenvertaisesta toimivuudesta eri ihmisryhmillä, kuten eri-ikäisillä, eri sukupuolta olevilla tai eri etnisistä taustoista tulevilla henkilöillä. Tähän liittyen on tärkeää tarkastella, miten teknologian kehityksessä ja käyttöönotossa voidaan varmistaa, ettei se johda syrjintään tai heikkoon turvaan tietyille käyttäjäryhmille.

Tässä insinöörityössä perehdytään älypuhelinten biometrisiin tunnistusmenetelmiin, niiden toimintaan, tietoturvahaasteisiin sekä tulevaisuuden kehityssuuntiin. Työssä tarkastellaan myös tunnistusmenetelmien luotettavuutta ja vertaillaan tunnistusjärjestelmien turvallisuutta eri arviointikriteerien avulla. Lisäksi käsitellään erilaisia keinoja, joilla tunnistusmekanismeja voidaan huijata ja selvitetään, millaisia ratkaisuja alalla kehitetään tietoturvan parantamiseksi. Lopuksi pohditaan biometristen tunnistusmenetelmien eettisiä kysymyksiä, kuten tietojen väärinkäyttöä, käyttäjien suostumusta ja demografisia haasteita. Insinöörityön tavoitteena on tarjota monipuolinen katsaus biometriseen tunnistautumiseen älypuhelimissa sekä sen vaikutuksiin tietoturvan näkökulmasta.

2 Älypuhelinten biometriset tunnistusmenetelmät

Biometriset tunnistusmenetelmät ovat keinoja, joilla henkilö voidaan tunnistaa jonkin fysiologisen ominaisuuden, kuten sormenjäljen, perusteella. Tunnistusmenetelmien juuret ovat 1800-luvun rikostutkinnan menetelmissä, erityisesti sormenjälkien luokittelussa ja nykyään tunnettu moderni biometria lähti voimakkaasti kehittymään 1990-luvulla. [1, s. 4.] Nykyään biometriaa käytetään laajalti paitsi rikostutkinnassa myös arkielämässä, kuten älypuhelimissa ja muissa henkilökohtaisissa älylaitteissa.

Biometriset tunnistusmenetelmät ovat tulleet osaksi jokapäiväistä elämää ja niiden käyttö yleistyy jatkuvasti. Älypuhelimissa biometriset tunnistusmenetelmät, kuten sormenjälkitunnistus ja kasvojentunnistus, tarjoavat käyttäjille helppokäyttöisen tavan suojata laitteensa. Tekniikoiden etuna on, että ne perustuvat henkilön yksilöllisiin ominaisuuksiin, joita on haastava väärentää.

Biometriset tunnistusmenetelmät voidaan tyypillisesti jakaa kahteen kategoriaan, fyysisiin menetelmiin ja käytöksellisiin menetelmiin. Tunnetuimmat tunnistusmenetelmät, sormenjälki- ja kasvojentunnistus, ovat esimerkkejä fyysisistä tunnistusmenetelmistä. Fyysisen ominaisuuden tunnuspiirteenä on, että ne perustuvat ihmisen vartalon muotoihin ja syntymästä asti oleviin biologisiin piirteisiin. Käytökseen perustuvat menetelmät ovat ihmisen itse opittuja piirteitä, jotka

voivat kuitenkin tietyissä tapauksissa hyödyntää myös fyysisiä ominaisuuksia. Käytökseen perustuvat tunnistusmenetelmät hyödyntävät esimerkiksi henkilön käsialaa ja ääntä. [2, s. 13; 3.]

Toisin kuin kirjoitetuissa salasanoissa biometrisessä tunnistautumisessa ei odoteta täydellistä vastaavuutta. Kun salasanoissa hyväksytään vain täydellinen vastaavuus, biometrisissä menetelmissä tavoitellaan vain hyvää vastaavuutta. Tämä johtuu siitä, että täydellistä vastaavuutta on hyvin vaikea saavuttaa. Esimerkiksi sormenjälkitunnistuksessa hiki ja sormen painalluksen paine vaikuttavat siihen, millainen sormenjäljen mallinnus on. [3.] Järjestelmän olisi kohtuutonta vaatia, että käyttäjän sormenjälki tulisi olla täysin identtinen alkuperäisen mallin kanssa vuodenajasta, lämpötilasta ja painalluksesta riippumatta. Se, kuinka paljon sormenjäljen tai muun biometrisen piirteen tulee vastata alkuperäistä mallia, riippuu laitteen sisäänrakennetuista määritelmistä [3].

Biometrisen järjestelmän toimintaperiaate koostuu lähtökohtaisesti kahdesta vaiheesta riippumatta siitä, mitä tunnistuskeinoa käytetään. Kun käyttäjä haluaa ottaa tunnistusmenetelmän ensimmäistä kertaa käyttöön, hän syöttää biometrisen tietonsa älypuhelimeen esimerkiksi sormenjälkisensorin kautta. Tämän jälkeen järjestelmä kerää tiedon sensorista ja käyttää sen algoritmin läpi, joka luo biometrisestä tiedosta matemaattisen mallin. Tämän jälkeen malli tallennetaan tietokantaan. [4.]

2.1 Sormenjälkitunnistus

Ihmisen sormenjäljet kehittyvät jo sikiövaiheessa. Ainutlaatuinen jälki muodostuu ihon korkeuseroista, eli kohoumista ja matalista kohdista (kuva 1). Sormenjälkien vahvuus on niiden oletettu yksilöllisyys, mutta se on myös sormenjälkitunnistautumisen suurin riski. Jos kyberhyökkääjä onnistuu kopiomaan älypuhelimen käyttäjän sormenjäljen, seuraukset voivat olla vakavat. [3.] Koska sormenjälkiä käytetään vielä nykypäivänäkin rikostutkinnassa, niiden päätyminen vääriin käsiin voi olla jopa kohtalokasta.

Kuva 1. Sormenjäljen kohoumat ja matalat kohdat [5].

Valtaosassa nykyajan matkapuhelimia on mahdollisuus tunnistautua käyttäjän sormenjäljellä. Käyttäjä voi itse määritellä, kuinka monta ja mitä sormea haluaa tunnistautumiseen käyttää. Ergonomisesta näkökulmasta voidaan olettaa, että oikea tai vasen peukalo, riippuen käyttäjän kätisyydestä, on yleisin sormi tunnistautumiseen. Yksityisyydensuojan kannalta sormenjälkitunnistautumisen hyvä ominaisuus on, että eri sormia voi käyttää eri järjestelmiin tunnistautuessa [1, s. 31]. Täten esimerkiksi pankkisovellukseen voi tunnistautua eri sormenjäljellä kuin puhelimen lukituksen voi avata.

Sormenjälkitunnistimet voidaan jakaa kahteen kategoriaan, kosketukseen perustuviin sensoreihin ja kontaktittomiin optisiin sensoreihin. Yleisesti älypuhelimissa käytetään eniten kosketussensoreita, joiden toiminta perustuu valon avulla digitaalisen kuvan ottamiseen sormenjäljestä. [6.] Täten voidaan huomata, miten esimerkiksi sormen painalluksen vahvuus vaikuttaa digitaaliseen kuvaan ja sen vertailuun alkuperäiseen malliin. Näin ollen voidaan ymmärtää, miksi biometrisessa tunnistautumisessa täydellistä vastetta ei voi odottaa. Kontaktittomia optisia sensoreita ei sen sijaan tavata älypuhelimissa liki ollenkaan, vaikka sensorin ensimmäinen versio kehitettiin jo vuonna 2005 [2, s. 15].

Kontaktittomien sensorien toiminta perustuu sormenjäljen tunnistamiseen valon takaisinheijastuksesta. Sensori kohdistaa valoa sormea kohti ja päättelee valon takaisinheijastuksesta, onko sormenjälki oikea. Jotkut järjestelmät hyödyntävät myös teknologiaa, jolla tunnistetaan, onko sormen pinnassa hikeä. Näin voidaan varmistaa, että sormi on elävän ihmisen. [6.]

2.2 Kasvojentunnistus

Ihmiset ovat pitkään tunnistaneet lajitoverinsa heidän kasvojenpiirteidensä perusteella, ja kasvojentunnistus onkin yksi vanhimpia tunnistusmenetelmiä, vaikka se on älypuhelimissa varsin uusi ominaisuus [3]. Kasvojentunnistuksesta on nopeasti tullut mahdollisesti suosituin biometrisen tunnistautumisen keino johtuen sen teknologian edullisuudesta, helppokäyttöisyydestä ja suhteellisen matalasta virheprosentista. Verrattuna sormenjälkitunnistuksen sensoreihin, kasvojentunnistus ei vaadi ulkoisia sensoreita tehden kasvojentunnistuksella varustettujen älypuhelimien valmistuksesta kannattavampaa. [7.] Älypuhelinvalmistaja Apple on jättänyt sormenjälkisensorin pois iPhone-älypuhelimistaan jo vuonna 2017 julkaistun iPhone X:n jälkeen ja korvannut sormenjälkitunnistautumisen kokonaan kasvojentunnistuksella. Poikkeuksena on vuonna 2020 julkaistu 2. sukupolven iPhone SE. [8; 9.]

Älypuhelinten kasvojentunnistus perustuu teknologiaan, jossa henkilöllisyys varmistetaan kasvonpiirteiden perusteella joko digitaalisen kuvan tai videosta pysäytetyn kuvaruudun avulla [10]. Yleisesti kasvojentunnistuksessa käytetään joko kamerapohjaista tunnistusta tai infrapunavaloon perustuvaa tunnistusta. Kameratunnistusta käyttävät älypuhelimet vaativat ensimmäistä kertaa tunnistusta käyttöön ottavaa käyttäjää kuvaamaan kasvonsa useasta eri suunnasta. Sormenjälkitunnistuksen tavoin tämän jälkeen kuvat syötetään algoritmiin, joka erottelee kasvojenpiirteet ja tallentaa ne laitteen muistiin. Infrapunatunnistuksen toimintaperiaatteena on ottaa käyttäjästä kaksiulotteisia kuvia infrapunavalolla, jolloin valaistusolosuhteiden ei tarvitse olla yhtä hyvät kuin kamerapohjaisessa tunnistuksessa. [11.]

Kasvojentunnistusteknologia ei suosiostaan huolimatta ole virheetön tai täydellinen teknologia. Kasvojentunnistuksella voi olla vaikeuksia tunnistaa käyttäjää erilaisissa valaistusolosuhteissa, sääolosuhteissa ja asusteissa. Käyttäjä saattaa muuttaa ulkonäköään silmälaseilla tai kasvattamalla parran, jolloin järjestelmä ei välttämättä enää tunnista kasvoja. [3.] Nykyään moneen älypuhelimeen voikin lisätä useamman kasvojentunnistusmallin, jolloin satunnaisesti silmälaseja käyttävä tunnistetaan sekä silmälasit päässä että ilman. COVID-19-pandemian aikana käyttäjien oli mahdollista lisätä itsestään kasvojentunnistusmalli suu-nenäsuojus kasvoillaan, jolloin älypuhelin todensi käyttäjän, vaikka puolet kasvoista oli peitossa. Tällöin laite vaati käyttäjää ottamaan suoran katsekontaktin kameraan ennen lukituksen avaamista.

2.3 Iiristunnistus

Iiris, eli värikalvo, on silmän pupillin ympärillä oleva värillinen osa, joka tunnetaan ainutlaatuisesta kuvioinnistaan. Iiriksen ero muihin biologisiin tunnisteisiin on sen poikkeuksellinen yksilöllisyys, mikä tekee siitä ihanteellisen biometrisen tunnistautumisen keinon. [10.] Jopa identtisillä kaksosilla on toisistaan poikkeavat iirikset, eivätkä heidän iiriksensä ole keskenään sen enempää samanlaisia kuin kahden täysin tuntemattoman ihmisen [12]. Iiriksessä on monia tunnistettavia piirteitä, mutta niistä mahdollisesti olennaisin on trabekulaarinen verkosto, joka on kudosverkko lähellä sarveiskalvon pohjaa. Kudoksen erityinen kuvio voi erottaa yhden henkilön toisesta. Tämä rakenteellinen satunnaisuus varmistaakin iiristunnistuksen ainutlaatuisuuden. [10.]

Iiristunnistus on osoittautunut yhdeksi tehokkaimmista biometrisen tunnistuksen muodoista sen matalan virheprosentin ansiosta. Ainutlaatuisen kuvioinnin lisäksi iiriksen hyviä puolia on, ettei sen kuvio riipu henkilön biologisesta sukupuolesta, etnisestä taustasta tai silmien väristä. Tämä tekee tunnistusmallin kouluttamisesta helppoa ja kustannustehokasta, sillä kouluttamista ei tarvitse toteuttaa ulkonäöllisesti monipuolisella henkilöotannalla. [13.]

Huolimatta iiristunnistuksen monista hyödyistä se ei silti ole saatavilla uusimmissa älypuhelinmalleissa. Tämä johtuu siitä, että vaikka teknologia on osoittanut hyvää suorituskykyä ihanteellisissa olosuhteissa, on sen tekninen toteutus haastavaa ja virheprosentti kasvaa suuresti, kun iiristä yritetään tunnistaa epäotollisissa olosuhteissa. Onnistunut iiristunnistus vaatii korkealaatuisia kuvia hyvissä olosuhteissa, mutta iiriksen pienen koon sekä kostean ja heijastavan silmämunan vuoksi se on vaikea saavuttaa. Myös silmäluomien ja silmäripsien aiheuttama mahdollinen näköeste sekä silmän heijastus, aiheuttavat ongelmansa täydellisen kuvan saavuttamiseen. [13; 14.] Älypuhelinvalmistaja Samsung on ainut, jonka useammassa vanhassa älypuhelinmallissa on ollut iiristunnistin, mutta sen käytöstä luovuttiin uudemmissa malleissa.

3 Tunnistusmenetelmien luotettavuuden vertailu

Biometriset tunnistusmenetelmät ovat kehittyneet nopeasti älypuhelinten kehittyessä. Kuitenkin eri menetelmien luotettavuus voi vaihdella merkittävästi. Tässä luvussa tarkastellaan eri tunnistusmenetelmien luotettavuutta. Vertailun avulla pyritään arvioimaan, kuinka hyvin menetelmät voivat suojata käyttäjien henkilökohtaisia tietoja ja mitä haasteita niiden käytössä saattaa ilmetä.

3.1 Yleisten arviointikriteerien vertailu

Lähteiksi on valikoitunut kaksi tutkimusta niiden samojen vertailukriteereiden ja pitkän aikavälin ansiosta. Tutkimusten välinen pitkä aikaväli tarjoaa mahdollisuuden vertailla menetelmien luotettavuuden kehitystä kymmenen vuoden aikana. Tutkimuksissa käsitellään useita eri biometrisiä piirteitä ja tunnistusmenetelmiä, mutta tässä luvussa keskitytään luvussa 2 esiteltyihin teknologioihin eli sormenjälkitunnistukseen, kasvojentunnistukseen ja iiristunnistukseen.

Biometrisiä piirteitä verrataan molemmissa tutkimuksissa seitsemään yleiseen arviointikriteeriin:

- universaalisuus
- ainutlaatuisuus
- pysyvyys
- kerättävyys
- suorituskyky
- hyväksyttävyys
- kiertäminen. [10; 15.]

Universaalisuus tarkoittaa biometrisen piirteen yleisyyttä populaatiossa ja kertoo, kuinka moni ihminen voi käyttää tunnistusmenetelmää [15]. Esimerkiksi voidaan pohtia, kuinka monella ihmisellä on sormenjäljet, ja näin voidaan arvioida kuinka moni ihminen voi käyttää sormenjälkitunnistinta. Ainutlaatuisuus kertoo, kuinka paljon henkilön biometrinen piirre eroaa toisen ihmisen samasta piirteestä, ja on oleellinen mittari tietoturvallisen tunnistautumisen kannalta [15]. Piirteen pysyvyydellä voidaan arvioida, pysyykö piirre samana tulevaisuudessakin. [15.]

Tunnistusjärjestelmän toteutettavuuden ja valmistushinnan kannalta oleellinen kriteeri on kerättävyys, joka ilmaisee, kuinka helppoa biometrisen piirteen kerääminen ja mittaaminen on. Suorituskyky kertoo, kuinka tarkka ja luotettava biometrisen piirteen tunnistusjärjestelmä on tunnistamisen kannalta. Suorituskyky on tärkeä mittari tietoturvallisuuden kannalta. Hyväksyttävyys ilmaisee ihmisten halukkuutta käyttää biometristä piirrettä tunnistautumiseen. Kriteeri ottaa huomioon muun muassa yksityisyyshuolet ja ihmisten tulkitseman hyödyllisyyden. Kiertäminen kertoo, kuinka helppoa tunnistusjärjestelmän huijaaminen ja kiertäminen on. Suorituskyvyn ja ainutlaatuisuuden ohella kiertäminen vaikuttaa vahvasti tietoturvaan ja onnistuneeseen tunnistautumisprosenttiin. [15.]

Alrawili, AlQahtani ja Khan [15] tekivät vuonna 2024 vertaillun, jonka perusteella (taulukko 1) voidaan tarkastella jokaisen jo esitellyn tunnistusmenetelmän vahvuuksia. Huomattakoon, ettei voida suoraan todeta arvon ”korkea” olevan hyvä

ja ”matala” huono. Arvojen merkityksellisyys vaihtelee arvioitavan kriteerin mukaisesti. Kun arvioidaan suorituskykyä, ”korkea” arvo paras, sillä se kertoo, että järjestelmä on luotettava, ja tämä vaikuttaa tietoturvallisuuteen positiivisesti. Sen sijaan kiertämisessä ”korkea” arvo kertoo, että järjestelmä on helppo kiertää, mikä vähentää tietoturvallisuutta.

Taulukko 1. Biometristen piirteiden vertailu arviointikriteerien avulla 2024 [15].

Biometrinen piirre	**Universaalisuus**	**Ainutlaatuisuus**	**Pysyvyys**	**Kerättävyys**	**Suorituskyky**	**Hyväksyttävyys**	**Kiertäminen**
Sormenjälki	Keskiverto	Korkea	Korkea	Keskiverto	Korkea	Keskiverto	Korkea
Kasvot	Korkea	Matala	Keskiverto	Korkea	Matala	Korkea	Keskiverto
Iiris	Korkea	Korkea	Korkea	Keskiverto	Korkea	Keskiverto	Matala

Taulukon perusteella voidaan päätellä, että iiristunnistus suoriutuu parhaiten yleisten arviointikriteerien vertailussa. Se saa parhaimman arvon viidessä kategoriassa seitsemästä sormenjälki- ja kasvojentunnistukseen verrattuna. Ainoastaan kerättävyydessä ja hyväksyttävyydessä kasvojentunnistus saa paremmat arvot piirteen helpon mitattavuuden, edullisemman hinnan ja käyttäjien hyväksynnän ansiosta.

Tutkimus ilmaisee hyvin biometristen tunnisteiden tämänhetkisen arvioinnin, mutta kehitystä olisi vaikea huomata ilman toisen tutkimusryhmän tekemää aiempaa vertailua. Meng, Wong, Furnell ja Zhou [10] tekivät vuonna 2014 tutkimuksen samoilla arviointikriteereillä, joka osoittaa, miten teknologian kehitys ja ihmisten mielipiteet ovat muokkautuneet kymmenen vuoden aikana (taulukko 2). Huomattakoon, että Mengin, Wongin, Furnellin ja Zhoun [10] tutkimuksen taulukossa kiertämisen kohdalla oleva arvo ”korkea” kertoo, että tunnistusjärjestelmää on vaikea huijata, kun Alrawilin, AlQahtanin ja Khanin [15]

tutkimuksessa tilanne oli päinvastainen. Vertailun helpottamiseksi taulukossa on sulkuihin merkitty arvo samalla näkökulmalla kuin vuoden 2024 tutkimuksessa. Lisäksi taulukkoon on merkitty asteriskillä (*) arvot, jotka eroavat vuoden 2024 tutkimukseen.

Taulukko 2. Biometristen piirteiden vertailu arviointikriteerien avulla 2014 [10].

Biometrinen piirre	**Universaalisuus**	**Ainutlaatuisuus**	**Pysyvyys**	**Kerättävyys**	**Suorituskyky**	**Hyväksyttävyys**	**Kiertäminen**
Sormenjälki	Keskiverto	Korkea	Keskiverto	Keskiverto	Korkea	Korkea*	Keskiverto*
Kasvot	Korkea	Matala	Keskiverto	Korkea	Matala	Korkea	Matala (Korkea)*
Iiris	Korkea	Korkea	Korkea/Keskiverto	Keskiverto/Matala	Korkea	Matala*	Korkea (Matala)

Mengin, Wongin, Furnellin ja Zhoun [10] arviointi perustuu kirjallisuuteen, verkkolähteisiin ja tutkimuksen kirjoittajien omiin kokemuksiin. Täten voidaan kriittisesti ajatella, etteivät tutkimukset ole suoraan verrattavissa toisiinsa, vaan tarjoavat enemmänkin pääpiirteittäistä apua teknologioiden kehityksen ja luotettavuuden vertailuun. Arviointikriteerit perustuvat yleisessä käytössä tapahtuvaan tunnistautumiseen, sillä esimerkiksi tunnistusjärjestelmän hyväksyttävyys voi tavallisella ihmisellä olla korkea, mutta korkean turvallisuustason laitoksissa matala [10].

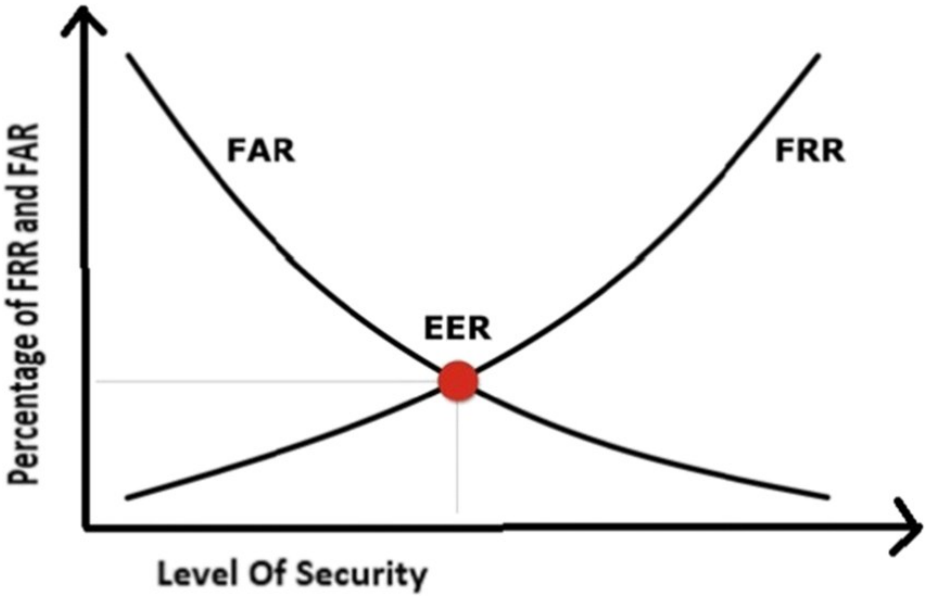
Yleisten arviointikriteerien vertailusta voidaan huomata, että sormenjälkitunnistautumisen hyväksyttävyys on laskenut kymmenen vuoden aikana arvosta korkea arvoon keskiverto [10; 15]. Kyberrikosten yleistyessä voidaan olettaa, että ihmisten halukkuus syöttää biometrisiä tietojaan kosketussensoreihin on vähentynyt. Sen sijaan iiristunnistuksen kehittyessä sen hyväksyttävyys on noussut arvosta matala arvoon keskiverto [10; 15]. Kehityksen syytä voi selittää

iiristunnistusteknologian kehittyminen ja korkea tietoturva. Mielenkiintoisena voidaan pitää myös kiertämisen arviointien eroa. Tutkimusten perusteella sormenjälkitunnistuksen huijaaminen olisi nykyaikana helpompaa, mutta kasvojentunnistuksen vaikeampaa [10; 15].

3.2 FAR- ja FRR-arvojen vertailu

Tunnistusmenetelmien vertailun perusteellisempaa analysointia varten tulee käsitellä niiden FAR (False Acceptance Rate) ja FRR (False Rejection Rate) -arvoja. FAR-arvo ilmaisee väärän tunnistamisen todennäköisyyttä, eli kuinka todennäköistä on, että tuntematon ihmisen pääsee kirjautumaan toisen ihmisen älypuhelimeen esimerkiksi sormenjäljellään. FRR-arvo ilmaisee taas oikean henkilöllisyyden hylkäyksen todennäköisyyttä, eli kuinka todennäköistä on, että oikea käyttäjä ei pääse kirjautumaan laitteelleen valitsemallaan biometrisellä tunnistusmenetelmällä. [15.]

Korkea FAR-arvo kertoo, ettei biometrinen järjestelmä ole kovin tietoturvallinen, kun taas korkea FRR-arvo voi johtaa käyttäjän turhautumiseen [16]. Täten mitä matalammat molemmat arvot ovat, sen parempi on järjestelmän suorituskyky ja tietoturva [15; 16]. Kuvasta 2 voidaan huomata, että molempien arvojen samanaikaista mataluutta on kuitenkin lähes mahdotonta saavuttaa, sillä toisen arvon laskiessa toinen välttämättä nousee. Tärkeintä onkin löytää tasapaino käytettävyyden ja tietoturvallisuuden välille. Tätä tasapainopistettä, jossa molemmat arvot ovat samat, kutsutaan EER (Equal Error Rate) -arvoksi. [16.]



Kuva 2. FAR- ja FRR-arvojen tasapainopiste EER [17, s. 27 733].

Alrawilin, AlQahtanin ja Khanin [15] teettämässä tutkimuksessa kerättiin biometristen tunnisteiden FAR- ja FRR-arvoja useista eri kirjallisuuslähteistä. Näiden lähteiden perusteella voitiin havaita, että kasvojentunnistuksella oli korkein FAR-arvo, vaihteluvälillä 0,1–1,0 %. Matalin vaihteluväli, 0,0001–0,01 %, oli iiristunnistuksella ja sormenjälkitunnistus oli näiden keskivaiheilla 0,01–0,1 %:n arvoillaan. Tarkastelemalla näitä vaihteluvälejä voidaan huomata jälleen iiristunnistuksen vahva tietoturvallisuus. Iiristunnistus tarjoaa myös matalimmat FRR-arvot vaihteluvälillä 0,1–0,5 %, kun kasvojentunnistuksella on korkeimmat arvot 1,0–5,0 %:n vaihteluvälillä. Sormenjälkitunnistus asettuu jälleen kahden muun biometrisen tunnistuskeinon välimaastoon 0,1–1,0 %:n FRR-arvollaan. [15.]

Biometristen tunnistuskeinojen vertailu erilaisten arviointikriteerien ja arvojen perusteella antaa pintapuolisen yleiskatsauksen niiden luotettavuuteen ja tietoturvallisuuteen. Kuitenkin kaikki tunnistuskeinot ovat alttiita kyberhyökkäyksille ja huijausyrityksille, eikä mikään keino ole täysin pitävä. Seuraavassa luvussa käsitellään, miten biometristä dataa suojataan ja millä keinoin biometrisiä tunnistusjärjestelmiä yritetään kiertää.

4 Tietoturva ja haavoittuvuudet

4.1 Biometrisen datan suojaus

Biometriseen tunnistukseen on liitettävissä monia erilaisia uhkakuvia, joista älypuhelimissa olennaisimpia ovat identiteettivarkaus, biometrisen tiedon vuotaminen ja sen luvaton myynti [1, s. 7]. Identiteettivarkaus tarkoittaa tilannetta, jossa rikollinen esiintyy toisena henkilönä tältä varastetun biometrisen datan tai muiden tunnistetietojen turvin [18]. Yksilön kannalta turvallisinta on, jos biometrinen tunnistautuminen on aina liitettynä fyysiseen tunnisteeseen, kuten avainkorttiin tai salasanaan. Tämä kaksivaiheinen tunnistautuminen tarjoaa vahvimman turvan identiteettivarkauden sattuessa, sillä rikollinen ei pääse luvattomasti käsiksi uhrin laitteisiin vain yhdellä tunnistetiedolla. [1. s. 8–9]

Biometristen tunnistetietojen tallentamisesta laitteen muistiin ei ole määritelty tarkkoja lakeja, joten älypuhelinten valmistajat määrittelevät itse, miten data tallennetaan ja suojataan. Määrittelyn helpottamiseksi on luotu käsite tietoturvalliselle datan säilyttämiselle laitteen sisällä. TEE (Trusted Execution Environment) -ympäristö kertoo, millaisessa arkkitehtuurissa salaista dataa säilytetään. TEE-ympäristö on tietoturvallinen ja erillinen alue laitteen pääprosessorin sisällä. Se hyödyntää sekä laitteiston arkkitehtuuria että ohjelmistoja arkaluontoisen datan suojaamiseen. [19.]

Yhdysvaltalaisen teknologiayrityksen Applen biometristen tunnistetietojen suojaus perustuu biometrisen tunnistimen ja Secure Enclave -suojausarkkitehtuurin toimimiseen erillään, mutta suojatussa keskinäisessä yhteydessä. Tunnistin kerää biometrisen tiedon, kuten sormenjäljen ja lähettää sen Secure Enclavelle, joka prosessoi, salaa ja tallentaa tiedon. Kun käyttäjä yrittää tunnistautua, Secure Enclave vertaa uutta biometristä tietoa tallennettuihin malleihin ja vahvistaa avataanko laite tai hyväksytäänkö toiminto, kuten maksutapahtuma. [20.] Secure Enclave suojaa biometriset tiedot, jotka ovat salattuja ja tallennettuina laitteeseen matemaattisessa muodossa kuvan sijaan, eikä niitä jaeta muihin palveluihin [21].

Älypuhelimissaan Android-käyttöjärjestelmää hyödyntävät yritykset eivät paljasta yhtä kattavasti biometrisen datan suojaus- ja tallennuskeinojaan kuin Apple. Etelä-Korealainen Samsung kertoo, että heidän laitteillansa käyttäjän biometristä mittauksia ei jaeta ja tiedot ovat tallennettuna laitteen Knox Vaultiin sellaisessa muodossa, josta ei voi jäljentää alkuperäistä biometristä kuvaa [22]. Knox Vault on Samsungin älypuhelimissa sisäänrakennettu laitteisto, joka suojaa käyttäjän arkaluontoisia tunnistetietoja, kuten salasanoja ja biometristä dataa. Knox Vault on osa Samsungin TEE-arkkitehtuuria. [23.]

Kiinalaiset älypuhelinvalmistajat Huawei ja Honor eivät jaa syvää tietoa suojausarkkitehtuureistaan, vaan molemmat mainitsevat biometrisen datan olevan suojattuna käyttäjän laitteen muistissa, ja ettei sitä tallenneta ulkopuolisiin palveluihin, kuten pilvipalveluihin [24; 25]. Honor takaa, että kasvojentunnistukseen käytettävä biometrinen data muunnetaan salattuun muotoon algoritmin avulla, eivätkä kolmannen osapuolen palvelut saa dataa käyttöönsä kasvojentunnistuksen yhteydessä. Myös sormenjälkitiedot ovat tallennettuna muunneltuina malleina paikallisesti laitteessa. [24.] Huawei mainitsee, että biometriset tiedot ovat tallennettuna laitteen TEE:hen [25].

4.2 Sormenjälkien väärentäminen

Sormenjälkitunnistuksen laaja levinneisyys ja aiemmin todettu korkea kiertämistaso tekevät sen alttiiksi useille hyökkäyksille. Yleisesti biometristä tunnistusjärjestelmää voi yrittää huijata eri vaiheissa tunnistautumista, joko suoralla tai epäsuoralla hyökkäystavalla. Sormenjälkitunnistautuminen on erityisen altis suoralle hyökkäykselle, eli sensorihyökkäykselle, sillä kosketussensorin kiertäminen ei vaadi kuin hyvin tehdyn kopion sormenjäljestä. [26.] Suora hyökkäys voidaan jakaa kahteen kategoriaan, väärentämis- ja muutoshyökkäyksiin. Väärentämishyökkäys tarkoittaa biometrisen piirteen, tässä tapauksessa sormenjäljen, korvaamista keinotekoisella asialla esimerkiksi tekosormella. Sitä pidetään yleisimpänä suoran hyökkäyksen keinona mobiililaitteissa. [27.] Muutoshyökkäyksessä hyökkääjä käyttää omaa muunneltua biometristä piirrettään päästääkseen biometrisen lukituksen ohi [26].

Sormenjälkitunnistuksen väärennyshyökkäyksistä on tehty monia testejä, ja väärennyshyökkäys on suosittu tutkimusaihe tekniikan tutkimustietokanta IEEE Xploressa. Hakusanalla ”fingerprint spoofing” (sormenjäljen väärennys) tietokanta antaa tulokseksi 741 aiheeseen eri tavoin liittyvää tutkimustekstiä. Tutkimuksissa käytettävät sormea jäljittelevät materiaalit vaihtelevat, mutta yleisesti menetelmät ovat samankaltaisia. Useimpien tutkimuksien lähtökohtana on luoda kopio käyttäjän sormenjäljestä eri materiaaleille ja yrittää avata sillä käyttäjän älypuhelimen näyttölukitus.

Erään väärennyshyökkäystä simuloivan tutkimuksen mukaan 16 eri materiaaliyhdistelmistä tehtyä sormenjälkimallinnusta 35:stä johtivat ainakin yhteen onnistuneeseen kirjautumiseen käyttäjän sormenjälkisuojattuun Android-käyttöjärjestelmälliseen älypuhelimeen. Järjestelmä tunnisti yhdeksän artefaktia, eli sormenjälkimallinnusta, aidoksi sormeksi, muttei hyväksynyt tunnistautumista. Tutkimuksen tekijät olivat aloittelijoita biometriassa, eikä heillä ollut aiempaa kokemusta sormenjälkien väärentämisestä. Mallinnuksissa käytetyt materiaalit olivat ostettavissa päivittäistavarakaupoista ja aikaa väärennösten tekemiselle ja testaamiselle oli vain 12 tuntia. Muottien luominen toteutettiin painamalla sormi valittuun pehmeään materiaaliin, joka koveni myöhemmin.

Muottien luomisen jälkeen itse artefakti painettiin muottiin ja käytettiin älypuhelimen kirjautumisyritykseen heti sen jälkeen. Tutkimuksen lopussa yksi artefakti saavutti 100 prosentin kirjautumisonnistumisprosentin. Artefaktin muotti oli tehty Siligumista, joka on silikonikittiä, ja itse artefakti oli algiinihappoa, jota käytetään esimerkiksi hammasmuoteissa. Yhdistelmä läpäisi kaikki kymmenen sillä teetettyä kirjautumisyritystä ja täten käyttäjän älypuhelin pystyttiin avaamaan ilman hänen omaa sormeaan. [28.] On kuitenkin tärkeää huomata, että 100 prosentin onnistumisprosentti saavutettiin vain yhdellä älylaiteella. Samaa Siligumin ja algiinihapon yhdistelmää yritettiin myös kahteen muuhun älypuhelimeen, mutta toisessa onnistumisprosentti oli 70 % ja toisessa 0 %. Merkittävin ero kolmen älypuhelimen välillä oli sormenjälkisensorin sijainti. Laiteessa, jolla 100 prosentin kirjautumisonnistuminen saavutettiin, sensori sijaitsi laitteen sivussa, kun muissa kahdessa laitteessa se sijaitsi laitteen edessä.

Muutoshyökkäyksiä ei ole tutkittu läheskään yhtä paljon kuin väärennyshyökkäyksiä. Muutamia tutkimuksia on kuitenkin löydettävissä sormenjälkien muokkaamisesta, joka voidaan tehdä poistamalla, vääristämällä tai jäljittelemällä niiden piirteitä. [26.] Näistä keinoista ainoastaan sormenjälkien piirteiden poistaminen ei vaadi kirurgisia toimenpiteitä. Piirteiden poistamisella tarkoitetaan kohoumien hävittämistä tai muokkaamista esimerkiksi viiltämällä, polttamalla tai hiomalla. Vääristäminen ja jäljitteleminen tapahtuvat kirurgisesti, sillä ne vaativat ihosiirtoa. Vääristämisessä ihonpalanen irrotetaan ja liitetään takaisin sormeen väärinpäin, jolloin sormen kohoumakuviosta tulee epätyypillinen. Jäljittelemisessä sen sijaan pyritän pitämään kohoumakuviointi mahdollisimman luonnollisena siirtämällä ihonpalanen osaksi sormenjälkeä. [29.]

4.3 Kasvojentunnistuksen huijaaminen

Kasvojentunnistusteknologian yleistyminen on johtanut siihen, että sen tietoturvaan kohdistuu yhä enemmän riskejä. Henkilön sormenjäljen ja iiriskuvioinnin päätyminen huijareille on huomattavasti hankalampaa kuin kasvonpiirteiden, koska valokuvan ottaminen henkilön kasvoista on yksinkertaisempaa kuin sormenjäljen kopioiminen ovenkahvasta. Lisäksi sosiaaliseen mediaan ladatut kuvat mahdollistavat, että ihmisten kasvonpiirteet ovat helposti saatavilla miltei kenelle tahansa. [30.]

Perinteiset kasvojentunnistusjärjestelmät ovat alttiita useille huijaustyyleille, eivätkä ne aina havaitse hyökkäysyrityksiä. Useat älypuhelinvalmistajat ovat lisänneet kasvojentunnistusteknologiaansa ”liveness detection” -tekniikan. Tekoälyä hyödyntävä tekniikka parantaa kasvojentunnistuksen tietoturvallisuutta analysoimalla kasvojen liikkeitä, mikä vaikeuttaa tiettyjä huijaamista. Se havaitsee silmänräpäytykset, pään liikkeet ja muut merkit, jotka todistavat, että käyttäjä on elossa. [31.]

Kuten sormenjälkihyökkäykssessä, myös kasvojentunnistukseen kohdistuvat hyökkäykset ovat pääsääntöisesti suoria väärennyshyökkäyksiä. Kun puhutaan kasvojentunnistukseen kohdistuvista hyökkäyksistä, puhutaan

väärennyshyökkäyksestä yleensä nimityksellä esityshyökkäys. Esityshyökkäykset voidaan luokitella usealla eri tavalla lähteestä riippuen. Yksi tapa jakaa hyökkäystyylit on luokitella ne käytetyn teknologian mukaisesti joko 2D- tai 3D-hyökkäyksiin. [32.]

4.3.1 2D-hyökkäykset

Kaksiulotteiset hyökkäykset, eli 2D-hyökkäykset, ovat tapoja, joissa älypuhelimen kameralle esitetään yksinkertainen kuva henkilön kasvoista. Yksi ensimmäisistä hyökkäyskeinoista on staattinen 2D-hyökkäys, jossa hyökkääjä näyttää paperilla tai digitaalisella näytöllä olevaa kuvaa uhrin kasvoista älypuhelimen kameralle ja täten ohittaa kasvojentunnistusjärjestelmän. Hyökkäystyyppi on erityisen tehokas vanhoissa 2D-kasvojentunnistusjärjestelmissä. [32.]

Vuonna 2023 Which?-kuluttajajärjestön teettämä tutkimus osoittaa, että useiden valmistajien Android-käyttöjärjestelmälliset älypuhelimet voidaan avata pelkällä tulostetulla kuvalla käyttäjän kasvoista. Tutkimuksessa testattiin 48 uutta älypuhelinta, joista 19 kappaletta, eli noin 40 prosenttia, oli huijattavissa yksinkertaisella staattisella 2D-hyökkäyksellä. Valokuvat tulostettiin tavalliselle tulostuspaperille, eivätkä ne olleet kovin hyvälaatuisia. Useimmat testin hylänneet laitteet kuuluivat edulliseen tai keskihintaiseen luokkaan, mutta joukossa oli myös kalliita älypuhelimia, kuten lähes 1 000 euron hintainen Motorola Razr 2022. [33.]

Motorolan älypuhelimista kaikkiaan neljä oli alttiita paperihyökkäykselle. Kokonaismäärällisesti huonoimman tuloksen teki kiinalainen Xiaomi, jonka seitsemän älypuhelinta oli huijattavissa. Nokian, Oppon ja Samsungin mallistoista kustakin kaksi älypuhelinmallia ei läpäissyt testiä. Lisäksi Honorilla ja Vivolla oli molemmilla yksi älypuhelinmalli, joka oli huijattavissa. Toisin kuin monet Android-laitteet, Applen älypuhelimet eivät olleet alttiita staattisille 2D-hyökkäyksille. Apple käyttää kasvojentunnistuksessaan 3D-syvyyskartoitusta, joka tekee paperihyökkäyksistä tehottomia. [33.]

Kehittyneet dynaamiset 2D-hyökkäykset, kuten videoväärennökset, tuovat mukanaan uusia haasteita. Näissä hyökkäyksissä käytetään uhrin kasvoista tallennettua videomateriaalia harhauttamaan järjestelmiä, jotka vaativat kasvojen liikkeitä, kuten silmänräpäytyksiä tai hymyä. Videoväärennyshyökkäykset pystyvät myös reaaliaikaisesti manipuloimaan videomateriaalia vastaamaan järjestelmän satunnaisesti asettamin tehtäviin. [32.]

4.3.2 3D-hyökkäykset

Kolmiulotteiset eli 3D-hyökkäykset voidaan jakaa 2D-hyökkäyksen tavoin staattisiin ja dynaamisiin hyökkäyksiin. Staattiset 3D-hyökkäykset ovat kehittyneet erityisesti 3D-tulostimien ansiosta, sillä niiden avulla voidaan luoda tarkkoja kolmiulotteisia kasvomalleja, joita voidaan käyttää huijaamaan kasvojentunnistusjärjestelmiä. [32.]

Vuonna 2018 tehdyssä tutkimuksessa brittiläinen Backface-yritys skannasi toimittajan kasvot 50 kameran avulla ja muutti kuvat kolmiulotteiseksi malliksi editointiohjelmassa. Kasvomalli tulostettiin kipsipohjaisesta materiaalista 3D-tulostimella ja viimeisteltiin, jolloin se saatiin muistuttamaan toimittajan kasvoja mahdollisimman tarkasti. Tämän jälkeen kasvomallia käytettiin testissä, jossa viiden eri älypuhelimen kasvojentunnistusta yritettiin huijata. Älypuhelimet oli iOS-käyttöjärjestelmällinen iPhone X ja Android-käyttöjärjestelmälliset LG G7 ThinQ, Samsung S9, Samsung Note 8 ja OnePlus 6. Testitulokset osoittivat, että kasvomalli avasi kaikki neljä Android-laitetta vaihtelevalla nopeudella. iPhone X puolestaan pysyi lukittuna eikä hyväksynyt kasvomallia, mikä viittaa siihen, että Applen Face ID -teknologia tarjosi ainakin vuonna 2018 paremman suojan. [34.]

Dynaamisiin 3D-hyökkäyksiin sopivien fyysisten kasvomallien rakentaminen on vielä nykypäivänä haastavaa ja kallista, mutta virtuaaliympäristöissä luodut digitaaliset kasvomallit voivat olla realistinen uhka tietyille 3D-kasvojentunnistusjärjestelmille. [32.] Syväväärennysteknologian myötä aidolta vaikuttavien kasvoanimaatioiden luominen on tullut helpommaksi. Teknologiaan perustuvat hyökkäykset voivat hyödyntää kehittyneitä tekoälymalleja, jotka mahdollistavat

kasvojen reaaliaikaisen manipulaation täten ohittaen ”liveness detection” -teknologian. [35.]

4.4 Epäsuorat hyökkäykset

Epäsuorat hyökkäykset voidaan jakaa kahteen kategoriaan riippuen siitä, onko tarkoituksena hyökätä kohdennetusti järjestelmän ohjelmistomoduuleihin vai niiden väliin [26]. Järjestelmän moduulien väliin kohdistuvassa hyökkäyksessä, eli toistohyökkäyksessä, älypuhelimen sensoria ei tarvita lainkaan vaan tunnistusjärjestelmään uudelleen lähetetään käyttäjän aiemmin siepattu biometrinen data [36]. Toistohyökkäykset ovat erityisen vaarallisia sillä ne mahdollistavat automaattisen laajamittaisen hyökkäyksen useaa uhria vastaan hyödyntämällä haittaohjelmia, jotka kaappaavat biometrisiä tietoja. Tunnistustapahtuman tietoturvallisuutta voi parantaa, jos käyttäjän biometrinen data sisältää tiedon, onko data saatu tunnistustapahtuman kanssa samassa hetkessä. Kuitenkin, jos hyökkääjällä on mahdollisuus manipuloida tätä varmistusprosessia, on sen tuoma hyöty turha. [37.]

Ohjelmistomoduuliin kohdistuva hyökkäys voi tarkoittaa esimerkiksi tietokantaan kohdistuvaa hyökkäystä tai haittaohjelman lisäämistä [27]. Tietokantahyökkäykset voivat sisältää olemassa olevien biometristen mallien muuttamista, muokkaamista tai poistamista. Biometristen tietojen saaminen tietokannasta vaatii kuitenkin laajaa tietämystä tunnistusjärjestelmän toimintamekanismeista. [38.] Kuten luvussa 4.1 todettiin, älypuhelinvalmistajat takaavat, että biometriset mallit ovat tallennettuna matemaattisessa muodossa tietoturvallisiin ympäristöihin, joten tallennustietoihin hyökkääminen on ymmärrettävästi vaikea toteuttaa.

Haittaohjelman lisääminen ohjelmistomoduuliin, joka on vastuussa biometristen piirteiden erottelusta tai vertailusta, voi tarkoittaa, että hyökkääjä pystyy manipuloimaan tunnistustietojen vahvistusta haluamallaan tavalla. Tietoturvariskiä kasvattaa kalasteluhyökkäykset, joissa käyttäjiä houkutellaan lataamaan haittaohjelmia, jotka mahdollistavat biometrisen tiedon keräämisen ja laitteen muiden osien, kuten kameran, etäkäytön. [27.]

5 Tulevaisuuden biometriset menetelmät

Ihmisen lukuisien biometristen ominaisuuksien ansiosta tunnistusmenetelmät eivät rajoitu vain edellä mainittuihin tunnetuimpiin biometrisiin keinoihin. Sormenjälkitunnistautumisen ja kasvojentunnistuksen varjoon on jäänyt useita eri fyysisiä ja käytöksellisiä menetelmiä. Älypuhelimissa ei ole käytössä kaikkia samoja biometrisen tunnistautumisen keinoja, joita esiintyy esimerkiksi kulunvalvonnassa. Tulevaisuudessa erilaisten tunnistusmenetelmien käyttö voi yleistyä myös älypuhelimissa tarjoten uusia mahdollisuuksia tietoturvan ja käytettävyyden kannalta.

5.1 Käytökselliset tunnistusmenetelmät

Biometrisiä tunnistuspiirteitä on melkein niin monta kuin ihmisillä on tunnistettavia piirteitä ja käytösmalleja. Erityisesti käytöksellisten tunnistusmenetelmien monipuolisuus tuo uusia mahdollisuuksia. Näitä ovat esimerkiksi allekirjoituksen tunnistaminen, kävelytunnistus, painallusdynamiikka ja elektrokardiogrammiset (EKG) signaalit [36; 39]. Lähteestä riippuen EKG-signaaleihin perustuva tunnistus voidaan luokitella myös kognitiiviseksi tunnistusmenetelmäksi, koska se yhdistää ihmiskehon fyysisen ominaisuuden eli sydämen sähköisen toiminnan henkilön käytökselliseen piirteeseen, esimerkiksi siihen, miten henkilö reagoi valokuviin [2, s. 2].

Käytökselliset tunnistusmenetelmät tuovat mukanaan useita etuja älypuhelimen tunnistautumiseen. Yksi merkittävimmistä eduista on menetelmien kustannustehokkuus verrattuna fyysisiin tunnistusmenetelmiin, jotka vaativat hintavia laitteistoja. Käytökselliset menetelmät voivat hyödyntää laitteisiin valmiiksi kuuluvia antureita kuten kosketusnäyttöä, mikrofonia ja kiihtyvyysantureita. [40].

Lisäksi käytökselliset tunnistusmenetelmät parantavat älylaitteiden turvallisuutta monikerroksisen tietoturvan avulla. Verrattuna perinteisen kirjoitetun salasanan kopioimiseen käyttäjän ainutlaatuisten käyttäytymismallien kuten kirjoitustyylin kopioiminen on hyvin hankalaa. Käytökselliset menetelmät ovat myös

käytettävyydeltään parempia, sillä käyttäjän ei tarvitse muistaa salasanoja tai suorittaa erillisiä tunnistautumistoimia. [40].

Tutkimuksissa on osoitettu, että napautuskuvioihin perustuva tunnistusmenetelmä on varteenotettava vaihtoehto sen korkean käyttäjätunnistustarkkuuden ansiosta. Käyttäjien näytön napautuskäyttäytyminen on yksilöllistä ja vaikeasti kopioitavaa. Tutkimuksessa analysoitiin 120 käyttäjältä saatuja 960 napautuskuviota optimaalisen toleranssirajan selvittämiseksi ja havaittiin, että paras tunnistustarkkuus saavutettiin raja-arvojen 0,02 % ja 0,06 % välillä. Tämän jälkeen testattiin napautuskuvioinnin kopioimista, jolloin ulkopuolinen henkilö yritti katsoa käyttäjän olan yli, kun tämä suoritti oikean kuvioinnin viisi kertaa. Seuraavaksi ulkopuolisen henkilön tuli yrittää kopioida käyttäjän napautuskuviota. Tulokset osoittivat, että vaikka hyökkääjä oli havainnut oikean käyttäjän napautuskuvion useita kertoja, kopiointiyritykset epäonnistuivat suurimmassa osaa testitapauksia. Tämä osoittaa, että napautuskuvioihin perustuva tunnistusmenetelmä tarjoaa vahvan suojan älypuhelimelle ja voi olla tehokas lisä nykyisiin käytöksellisiin tunnistusmenetelmiin. [41.]

Tulevaisuudessa käytökselliset biometriset menetelmät voivat mahdollistaa jatkuvan tunnistautumisen, jolloin käyttäjän henkilöllisyys varmennetaan jatkuvasti laitteen käytön aikana. Tämä lisää tietoturvaa verrattuna muihin menetelmiin, joissa tunnistautuminen tapahtuu vain laitetta avatessa. [40.] Jatkuva tunnistautuminen voi tapahtua ilman käyttäjän aktiivista osallistumista, jolloin käyttäjän käytökselliset biometriset piirteet, kuten näytön kosketuskäyttäytyminen, kerätään ja analysoidaan laitteen normaalin käytön aikana. Käyttäjä voi vaihtaa sovelluksesta toiseen ilman, että tunnistautumisprosessi keskeytyy, mikä tekee menetelmästä huomaamattoman ja helppokäyttöisen. Jos tunnistautumisprosessi havaitsee epänormaalia käyttäytymistä, se voi pyytää käyttäjältä lisävarmennusta tai estää pääsyn laitteeseen. [42.]

Kokeellisten tulosten perusteella jatkuvan tunnistautumisen menetelmä voi saavuttaa matalan virhetason. Kosketuskäyttäytymiseen perustuvan tunnistautumisen EER-arvo oli 0,75 % ja liikekäyttäytymiseen perustuva arvo oli 2,14 %. [42.]

Arvot ovat suurin piirtein samalla tasolla kuin kasvojentunnistuksen arvot, joita esiteltiin luvussa 3.2.

Lisäksi tutkijat ovat kehittäneet hengityksen aiheuttaman ilman turbulenssin käyttöä biometristenä tunnistusmenetelmänä älypuhelimissa. Tutkimuksen mukaan tekoäly pystyy tunnistamaan yksilön hengityksen yli 97 prosentin tarkkuudella. Malli kykenee tunnistamaan ihmisen hengityksen ainutlaatuisen kuvion, joka johtuu ihmisen ylähengitysteiden rakenteellisista eroista. Yksi menetelmän eduista on, että se toimii vain elävillä henkilöillä toisin kuin esimerkiksi sormenjälkitunnistus, joka voi toimia myös kuolleella henkilöllä. [43.]

5.2 Fyysiset tunnistusmenetelmät

Uusia fyysisiä tunnistusmenetelmiä ei ole tutkittu tai kehitetty samaa tahtia kuin käytöksellisiä menetelmiä. Uudet fyysiset tunnistusmenetelmät kohtaisivat mitä todennäköisemmin samat heikkoudet kuin sormenjälki- ja kasvojentunnistus. Kuitenkin on olemassa tunnistusmenetelmiä, jotka ovat käytössä muualla kuin älypuhelimissa.

Verkkokalvontunnistus on biometrinen tunnistusmenetelmä, joka perustuu ihmisen silmän verkkokalvon ainutlaatuisiin verisuonikuvioihin. Verkkokalvontunnistusta ei tule sekoittaa aiemmin käsiteltyyn iiristunnistukseen, vaikka molemmat menetelmät perustuvat ihmisen silmän tunnistamiseen. Iiris, eli värikalvo, sijaitsee silmän etuosassa, kun taas verkkokalvo on silmän takaosassa. [10.]

Verkkokalvontunnistus tarjoaa erittäin korkean tietoturvallisuustason, sillä verkkokalvon rakenne on jokaisella ihmisellä ainutlaatuinen, ja tämä tekee sen väärentämisen lähes mahdottomaksi [10; 39]. Käytännössä käyttäjä asettaa paljaan silmänsä lähelle verkkokalvon tunnistavaa skanneria ja katsoo määrättyä pistettä 10–15 sekunnin ajan. Menetelmän epäkäytännöllisyyden ja laitteiston korkean hinnan takia sitä ei ole käyttöönotettu älypuhelimiin, vaan menetelmää hyödynnetään pääasiassa korkean turvatason ympäristöissä. [10.]

Toinen kehittynyt fyysinen tunnistusmenetelmä on kämmenen suonikuvaus. Tunnistusmenetelmä perustuu kämmenen verisuoniston ainutlaatuiseen kuvioon, joka kuvataan kontaktittoman infrapunavalon avulla. Infrapunavalo pystyy havaitsemaan vain verisuonet, joiden sisällä kulkee hapetonta hemoglobiinia. Tämän ansiosta vain suoniverkosto näkyy laitteelle samalla, kun muut käden kudokset jäävät näkymättömiksi. Tunnistukseen käytettävän skannerin toimintaperiaatteena on tallentaa yli viisi miljoonaa datapistettä jokaisella kuvauksella, mikä parantaa tunnistuksen tarkkuutta ja luotettavuutta. [44.]

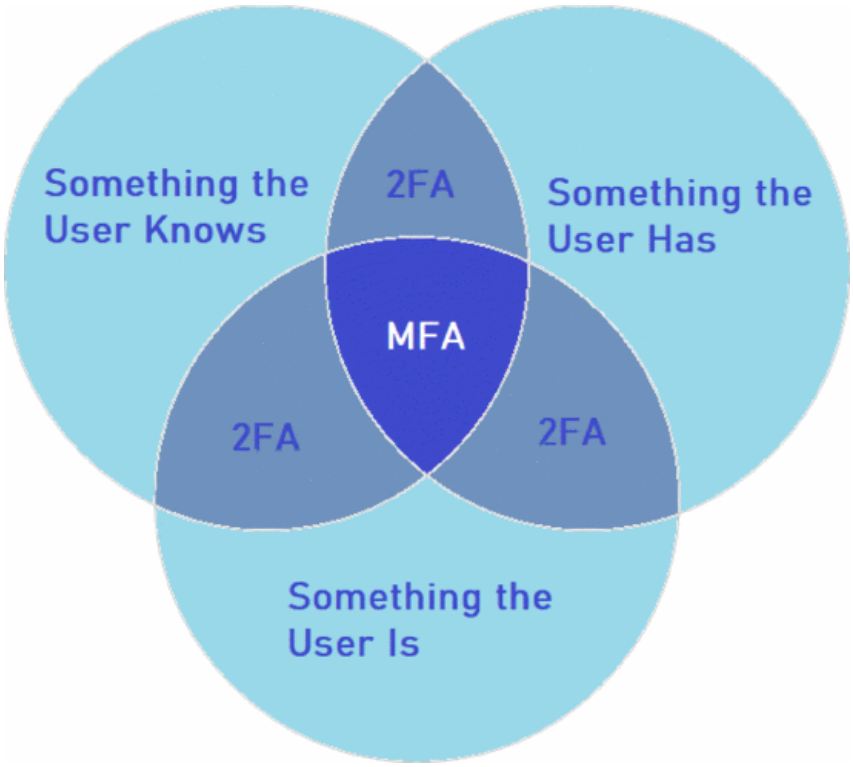
Kuten verkkokalvontunnistus myös kämmenen suonikuvaus tarjoaa erittäin vahvan tietoturvan. Koska verisuonisto sijaitsee ihon alla, on sen väärentäminen lähes mahdotonta [44]. Suonikuvioita ei voi myöskään jättää ovenkahvaan kuten sormenjälkeä tai saada selville sosiaalisen median kuvasta. Lisäksi kämmenen suonirakenne myös säilyy muuttumattomana läpi ihmisen elämän, mikä tarkoittaa, että järjestelmä pystyy tunnistamaan käyttäjän myös tämän ikääntyessä [44].

Korvatunnistus on vielä tuntematon, mutta kehittyvä biometrisen tunnistautumisen keino. Toisin kuin henkilön kasvot, korvan muoto ja rakenne säilyvät lähes muuttumattomina ajan kuluessa. Korvatunnistusta voidaan käyttää myös muiden tunnistusmenetelmien kanssa tilanteissa, joissa kasvot ovat peitetty tai muita biometrisiä tietoja ei ole saatavilla. Tunnistaminen perustuu joko 2D-kuviin tai 3D-pistepilviin, joiden avulla voidaan analysoida korvan piirteitä ja verrata niitä aiemmin tallennettuihin malleihin. [45.] On kuitenkin syytä pohtia, miten teknologia olisi sovellettavissa älypuhelinten tunnistusmenetelmäksi ja kuinka käytettävä se lopulta olisi.

5.3 Biometrinen yhdistelmätunnistautuminen

Käyttäjätunnistautumisen teknologiat voidaan jakaa kolmeen kategoriaan, jotka perustuvat siihen, mitä käyttäjä tietää, mitä käyttäjällä on ja mitä käyttäjä on. Jotain mitä käyttäjä tietää -kategoriaan kuuluvat perinteiset salasanat, PIN-koodit ja pääsykuviot. Jotain mitä käyttäjällä on -kategoriaan kuuluvat fyysiset esineet,

kuten salasanageneraattorit, tunnistekortit ja tekstiviestitse lähetetyt kertakäyttöiset salasanat. Jotain mitä käyttäjä on -kategoriaan kuuluvat fyysisen ja käytöksellisen tunnistamisen keinot, kuten sormenjäljet ja napautuskäyttäytymisen. Yhdistelemällä useita näiden kategorioiden keinoja osana tunnistamisprosessia voidaan puhua yhdistelmätunnistautumisesta. Yhdistelmätunnistautuminen voidaan jakaa vielä kaksivaiheiseen tunnistautumiseen (2FA) ja monivaiheiseen tunnistautumiseen (MFA) riippuen siitä, yhdistääkö tunnistautuminen kahden vai kaikkien kolmen kategorian keinoja (kuva 3). [40.]



Kuva 3. Tunnistautumisen kolme kategoriaa ja niiden yhdistelmät [40].

Kaksivaiheinen tunnistautuminen on tehokasta, kun se yhdistää sekä fyysisen että käytöksellisen tunnistautumisen keinot [46]. Yksittäisissä tunnistusmenetelmissä väärien hyväksymisten (FAR) ja väärien hylkäysten (FRR) arvot voivat olla korkeampia ympäristöolosuhteiden vuoksi, mutta yhdistelmätunnistuksessa yhden menetelmän heikkoudet voidaan kompensoida toisen vahvuuksilla. [47.] Kun kasvojentunnistukseen yhdistetään äänentunnistus tai silmän liikkeiden

analysointi, järjestelmä voi tunnistaa käyttäjän luotettavimmin erilaisissa olosuhteissa, mikä parantaa sekä tietoturvaa että käyttäjäkokemusta.

Kasvojen- ja äänentunnistuksen yhdistäminen on osoittanut parantavan biometrisen tunnistautumisen tarkkuutta ja luotettavuutta matalilla FAR- ja FRR-arvoilla. Kaksivaiheinen tunnistus hyödyntää kasvojenpiirteitä, kuten silmien, nenän ja suun muotoa ja äänentunnistusta, joka analysoi äänen taajuutta, rytmiä ja äänenvoimakkuutta. Teknologisesti menetelmät voivat toimia joko rinnakkain tai toisiaan täydentäen. Rinnakkaisessa tunnistuksessa molemmat menetelmät suorittavat tunnistamisprosessin itsenäisesti ja käyttäjän on läpäistävä molemmat varmennukset. Täydentävässä tunnistuksessa toinen menetelmä voi vahvistaa toisen epävarman tuloksen esimerkiksi tilanteessa, jossa kasvojentunnistusta haittaa heikko valaistus, mutta äänentunnistus antaa selkeän tuloksen. [47.]

Toiminnallisesti tunnistautumisprosessissa käyttäjä lausuu ennalta määrätyn numerosarjan samanaikaisesti kuin järjestelmä tunnistaa tämän kasvoja. Jos molemmat tunnistusmenetelmät tuottavat riittävän korkean osumatarkkuuden, tunnistautuminen hyväksytään. Mikäli vain toinen menetelmistä antaa luotettavan tuloksen, tunnistautuminen hylätään. [47.]

Uudet tutkimukset ovat kehittäneet haaste-vastaus-protokolliin (CR) perustuvia biometrisiä tunnistusmenetelmiä, joissa käyttäjän tulee reagoida satunnaiseen tunnistushaasteeseen. Haasteena voi olla esimerkiksi lausua ääneen tunnistusjärjestelmän määrittelemät numerot, jolloin järjestelmä varmistaa sekä numeroiden paikkaansapitävyyden että käyttäjän äänen. Erityisesti älypuhelimiin on kehitetty uusi biometrinen CR-tunnistautumisjärjestelmä, joka hyödyntää käden puristusvoimaa (PCR). Menetelmä analysoi käyttäjän kämmentä ultraäänisignaalilla ja mittaa puristusvoiman lisäksi käden geometriaa ja kämmenen kokoa. PCR-pohjainen tunnistus on todettu turvalliseksi, sillä käyttäjän kehon rasvaprosenttia ja kämmenen puristusvoimaa on vaikea jäljitellä. Lisäksi jokainen tunnistautumiskerta on ainutlaatuinen, koska järjestelmä muuttaa ultraäänisignaalin

taajuutta jokaisella käyttökerralla. PCR-tunnistus voidaan toteuttaa ilman erillistä laitteistoa kaikilla laitteilla, joissa on kaiutin ja mikrofoni. [48.]

PCR-tunnistautuminen on testattu kolmella erilaisella hyökkäyksellä: väärennyshyökkäyksellä, toistohyökkäyksellä ja esityshyökkäyksellä. Esityshyökkäysyrityksissä tunnistusjärjestelmän 6-numeroisen koodin FAR-arvo oli vain 1 % ja FRR-arvo 0,4 %, mikä tekee siitä erittäin luotettavan. Myös kehittyneimmissä hyökkäyksissä, joissa hyökkääjät yrittävät matkia käyttäjän käden otetta, FAR-arvo oli alhainen (2,6 %). PCR-tunnistautuminen osoitti hyvää suojaa myös toistohyökkäyksiä vastaan (FAR 0 %) johtuen jokaisen tunnistautumiskerran ainutlaatuisuudesta. Väärennetyillä silikonisilla käsillä ja 3D-tulostetuilla käsillä tehdyissä hyökkäyksissä järjestelmä ei saavuttanut yhtä matalia arvoja, sillä 3D-tulostetut kädet pystyivät jäljittelemään käyttäjän otetta tarkemmin (FAR 3,8–7,5 %). [48.]

Yhdistelmätunnistautuminen tarjoaa vahvemman suojan älypuhelimelle, ja merkitystä korostetaan myös Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen suosituksissa. Kaksivaiheinen ja monivaiheinen tunnistautuminen tekevät tilien kaappaamisesta huomattavasti vaikeampaa kahden tai useamman tunnistautumistavan ansiosta. Kyberturvallisuuskeskuksen mukaan monivaiheinen tunnistautuminen on suositeltavaa ottaa käyttöön erityisesti sähköpostissa ja sosiaalisen media tileillä tietoturvan parantamiseksi. [49.] Myös organisaatioiden tietoturvakäytännöissä Kyberturvallisuuskeskus suosittelee vahvojen salasanojen sekä monivaiheisen tunnistautumisen on käyttöönottoa [50].

Vaikka yhdistelmätunnistautuminen ei täysin poista tietoturvariskejä, se estää tehokkaasti satunnaisia tilikaappausyrityksiä ja tekevät hyökkääjän työn huomattavasti vaikeammaksi. Näiden suositusten mukaisesti yhdistelmätunnistautuminen on tällä hetkellä yksi parhaista tavoista varmistaa käyttäjän turvallinen tunnistautuminen. [50.]

5.4 Biometria ja tekoälyn kehitys

Tekoälyn hyödyntäminen biometrisissä tunnistusjärjestelmissä on yleistynyt merkittävästi, sillä se tarjoaa mahdollisuuden parantaa järjestelmien tietoturvaa tunnistamalla käyttäjät tarkasti. Tekoälyn hyödyntäminen perustuu koulutettuihin algoritmeihin, jotka käsittelevät suuria tietomääriä tehokkaasti. Kasvojentunnistuksessa tekoälyä voidaan hyödyntää tunnistusprosessin lisäksi algoritmien jatkuvaan kehittämiseen. Tekoälyä hyödyntämällä tunnistusalgoritmit pystyvät mukautumaan ajan myötä käyttäjän ulkonäön muutoksiin ja kehittämään tunnistamistarkkuuttaan. Sormenjälkitunnistuksessa tekoäly tunnistaa sormien kuvioinnit ja vertailee niitä alkuperäisiin malleihin. Myös yhdistelmätunnistautumisen monet vaiheet olisivat vaikeasti toteutettavissa ilman tekoälyä. [51.]

Tekoälyn hyödyntämisessä on myös haasteita. Mustan laatikon ongelmasta puhutaan, kun tekoälyn algoritmien päätöksentekoprosessi on vaikeasti ymmärrettävää [51]. Ongelmaa esiintyy erityisesti järjestelmissä, joissa hyödynnetään laajoja tietoaineistoja. Jos päätöksenteko ei ole läpinäkyvää, herää käyttäjille kysymys järjestelmien luotettavuudesta. [52.] Haasteen ratkaisuksi on kehitetty selittävä tekoäly (XAI), jonka tavoitteena on tehdä tekoälyn algoritmien päätöksistä ymmärrettäviä ja jäljitettäviä. Selittävä tekoäly mahdollistaa, että käyttäjät ja järjestelmien kehittäjät saavat tiedon siitä, mihin tekoäly perustaa vastauksensa. [51]

Selittävän tekoälyn soveltaminen biometrisiin järjestelmiin on yleistynyt, sillä syväoppimiseen perustuvat tunnistusmallit voivat kärsiä mustan laatikon ongelmasta. XAI:n avulla kasvojentunnistusjärjestelmissä voidaan hyödyntää visuaalisia ja ominaisuuspohjaisia selityksiä, jotka korostavat tunnistustuloksiin vaikuttavia kasvojen alueita. Käytännössä XAI korostaa esimerkiksi värien avulla ne kohdat henkilön kasvoissa, jotka vaikuttavat tunnistustulokseen. Tämä mahdollistaa tunnistusmallien arvioinnin ja mahdollistaa järjestelmän virheiden tunnistamisen. [53.]

Kasvojentunnistuksen lisäksi XAI:ta voidaan hyödyntää muissakin biometrisissä menetelmissä, kuten sormenjälki- ja verkkokalvotunnistuksessa. Erityisesti yhdistelmätunnistautumisessa XAI:n avulla voidaan selittää, miten eri tunnistustavat vaikuttavat lopulliseen päätöksentekoon. Tulevaisuudessa selittävän tekoälyn kehitys voi edistää biometrisen tunnistuksen eettisyyttä ja luotettavuutta. [53.]

6 Eettiset näkökulmat biometrisiin tunnistusmenetelmiin

6.1 Lainsäädäntö ja suostumus

Euroopan Unionin (EU) tekoälylakia alettiin osittain soveltamaan 2. helmikuuta 2025. Sen tavoitteena on pyrkiä estämään tekoälyn väärinkäyttö erityisesti suuren riskin tilanteissa, joissa voi ilmentyä biometrisen tiedon perusteella tapahtuvaa luokittelua. [54.] Toistaiseksi laki ei kuitenkaan koske älypuhelinten biometristä tunnistautumista, sillä laki poissulkee järjestelmät, joiden tarkoitus on biometrinen todennus [55].

> Näihin eivät kuulu tekoälyjärjestelmät, joita on tarkoitus käyttää biometriseen todennukseen, joka käsittää tunnistautumisen, ja joiden ainoana tarkoituksena on vahvistaa, että tietty luonnollinen henkilö on se henkilö, joka hän väittää olevansa, sekä vahvistaa luonnollisen henkilön henkilöllisyys ainoastaan jonkin palvelun käyttämiseksi, laitteen lukituksen poistamiseksi tai valvottuun tilaan pääsemiseksi. [55.]

Käyttäjän biometriset tiedot kuuluvat EU:n yleisen tietosuoja-asetuksen (GDPR) mukaan erityisten henkilötietojen ryhmään. Ryhmään kuuluvien henkilötietojen käsittely on lähtökohtaisesti kiellettyä, ellei käsittelylle ole säädetty poikkeusta. Jos käyttäjä on antanut suostumuksen biometrisen tiedon käsittelyyn, on tietojen käsittely GDPR:n mukaan hyväksyttävää. [56.] Käyttäjän antama suostumus on pätevä, jos käyttäjä on tietoinen kerättävän tiedon käyttötarkoituksesta, suostumuksen peruuttaminen on yhtä helppoa kuin sen antaminen ja suostumus on selkeä tahdonilmaisu. Selkeäksi tahdonilmaisuksi ei riitä esimerkiksi valmiiksi hyväksytty ruutu tai jonkin teon tekemättä jättäminen. [57.] Käytännössä älypuhelimen käyttäjät eivät välttämättä saa kattavaa tietoa siitä, miten

heidän biometrisiä tietojansa käytetään ja tallennetaan rekisteröitymisvaiheessa. Monissa älypuhelimissa biometrinen tunnistautuminen on oletusasetus ja käyttäjille ei aina tarjota selkeää vaihtoehtoa ilman biometriaa toimiville kirjautumismenetelmille.

Kuitenkin, koska älypuhelinvalmistajat takaavat, että käyttäjän biometriset tiedot ovat tallennettuna vain paikallisesti älypuhelimeen, tietojen hallinta on käyttäjällä. Täten valmistajien ei tarvitse suoraan noudattaa GDPR:n säädöksiä. [58.] GDPR:n mukaisesti asetusta ei sovelleta sellaisten henkilötietojen käsittelyyn ”jonka luonnollinen henkilö suorittaa yksinomaan henkilökohtaisessa tai kotitalouttaan koskevassa toiminnassa” [59]. Nähtäväksi jää, tulkitaanko GDPR:ää tilanteissa, joissa biometristä tunnistautumista käytetään esimerkiksi työnantajan tarjoamalla työpuhelimella.

6.2 Käyttäjien suhtautuminen ja luottamus

Vaikka älypuhelinten biometriset tunnistusmenetelmät tarjoavat käyttäjille tasapainon mukavuuden ja turvallisuuden välillä, tutkimukset osoittavat, että käyttäjät eivät ole aina täysin tietoisia tunnistautumiseen liittyvistä riskeistä. Käyttäjät luottavat älypuhelinvalmistajiin, mutta luottamus perustuu usein rajalliseen ymmärrykseen siitä, miten heidän biometrisiä tietojansa käsitellään ja suojataan. [60.] Teknologian hyväksymistä kuvataan teknologian omaksumismallilla (TAM), joka kuvaa, miten käyttäjät suhtautuvat uuteen teknologiaan perustuen sen hyödyllisyyteen ja käytettävyyteen. TAMin mukaan käyttäjien käsitys teknologian hyödyllisyydestä ja käytettävyydestä vaikuttavat myönteisesti heidän asenteeseensa teknologian käyttöä kohtaan. [61.]

Tutkimukset osoittavat, että käyttäjien luottamus perustuu käsitykseen turvallisuudesta ja yksityisyydestä. Käyttäjä jatkaa biometrisen tunnistautumisen käyttöä, jos hän kokee, että hänen tietonsa ovat turvassa ja tietoja käsitellään vastuullisesti. Toisaalta jos käyttäjä kokee, etteivät hänen biometriset tietonsa ole turvassa, hän saattaa olla haluttomampi ottamaan tunnistautumista käyttöön.

Tutkimuksen mukaan erityisesti nuoret sormenjälkitunnistuksen käyttäjät eivät tiedosta tunnistautumiseen liittyviä riskejä. [60.]

Kasvojentunnistuksen kannalta tutkimukset ovat osoittaneet, että käytettävyys ja tunnistuksen käytöstä koettu nautinto vaikuttavat merkittävästi kasvojentunnistuksen käyttäjiin, sillä käyttäjälle miellyttävä suunnittelu lisää käyttökokemusta. Lisäksi käyttäjien luottamus järjestelmää kohtaan vaikuttaa merkittävästi sen houkuttelevuuteen. [61.]

On tärkeää, että käyttäjille tarjotaan kattavaa ja ymmärrettävää tietoa biometrisen tunnistautumisen toiminnasta ja sen riskeistä. Käyttäjille tulisi antaa selkeät vaihtoehdot, jotka mahdollistavat biometristen tietojen hallinnan, kuten mahdollisuuden peruuttaa suostumus ja valita toisia kirjautumistapoja. Käyttäjien tietoisuuden lisääminen ja läpinäkyvä tiedottaminen ovat keskeisiä keinoja, joilla voidaan varmistaa, että biometrisen tunnistautumisen käyttö pysyy turvallisena ja eettisesti hyväksyttävänä.

6.3 Syrjintä ja tarkkuuserot

Biometrisen tunnistusteknologian yleistyminen on tuonut mukanaan sekä hyötyjä että haasteita. Vaikka useat tunnistusjärjestelmät tarjoavat nopean ja vaivattoman tavan tunnistaa käyttäjiä, niiden oikeudenmukaisuus ja saavutettavuus kaikille käyttäjäryhmille ei ole taattua.

Tutkimuksissa on havaittu, että kasvojentunnistusjärjestelmät eivät toimi yhtä luotettavasti kaikille ihmisille, joka johtaa syrjiviin lopputuloksiin. Epätasa-arvo ilmenee esimerkiksi siinä, että tietyt etniset ryhmät ja sukupuolet kohtaavat suuremman riskin virhetunnistuksille kuin muut. [62.] Tästä syystä on tärkeää tarkastella kriittisesti muun muassa kasvojentunnistuksen algoritmeja ja koulutusmateriaalia sekä kehittää teknologioita, jotka ovat yhdenvertaisia ja saavutettavia kaikille käyttäjille. Huomioin arvoista on, että suurin osa tutkimuksista keskittyy kasvojentunnistusteknologiaan yleisellä tasolla eikä suoraan älypuhelimissa oleviin kasvojentunnistusjärjestelmiin. Lisäksi muihin biometrisiin

tunnistuspiirteisiin, kuten sormenjälkitunnistukseen, ei löydy yhtä kattavaa tutkimusaineistoa.

Erityisesti kasvojentunnistuksen tarkkuutta on tutkittu eri väestöryhmillä. Kasvojentunnistuksen epätasa-arvoiset tulokset ovat erityisen merkittäviä, kun tunnistaminen tapahtuu näkyvän valon spektrillä, jossa ihonväri ja valaistusolosuhteet vaikuttavat tunnistusjärjestelmien tarkkuuteen. Tutkimukset ovat osoittaneet, että henkilöt, joilla on tummempi ihonsävy sekä naiset kohtaavat useammin virhetunnistuksia kuin vaaleaihoiset ja miehet. Tämä johtuu osittain siitä, että monet tunnistusalgoritmit on koulutettu epätasapainoisilla aineistoilla, joissa vaaleaihoiset ja miehet ovat yliedustettuina muihin väestöryhmiin verrattuna. [62; 63.]

Sukupuolten väliset erot kasvojentunnistuksen tarkkuudessa eivät selity pelkästään algoritmien koulutukseen käytettyjen kuvien eroilla. Tutkimuksissa on havaittu, että naisten kuvissa esiintyy useammin hymyilyä, suurempia pään kulmaeroja sekä otsaa peittäviä hiuksia. Kun koulutusaineistoa muokattiin siten, että mukana oli vain neutraalikasvoisia henkilöitä, pään kulmaerot poistettiin ja hiukset siirrettiin pois otsalta, kasvojentunnistuksen tarkkuus parani, mutta muokkauksista huolimatta kasvojentunnistus tunnisti miehet silti naisia tarkemmin. Lopuksi kasvojentunnistusjärjestelmää testattiin tasapainoisella koulutusaineistolla, jossa sukupuolet olivat yhtä paljon edustettuina, mutta tästä huolimatta tunnistustarkkuuden ero säilyi. [63.]

Tulevaisuudessa väestöryhmien välisten virhetunnistusten määrää voidaan vähentää. Eräässä tutkimuksessa on havaittu, että lähi-infrapunaspektrin käyttö kasvojentunnistuksessa on osoittautunut lupaavaksi keinoksi vähentää väestöryhmien välisiä virhetunnistuksia. Infrapunavalossa tehty kasvojentunnistus on vähemmän altis ihonvärin ja valaistuksen vaihtelulle, mikä voi parantaa järjestelmien yhdenmukaisuutta. Tutkimuksen perusteella väestöryhmien väliset tarkkuuserot pienenevät huomattavasti infrapunateknologialla tehtyihin tunnistuksiin verrattuna perinteisiin näkyvän valon kameroihin. [62.]

Uudet tutkimukset viittaavat siihen, että teknologian kehityksellä on keskeinen rooli biometristen tunnistusjärjestelmien syrjinnän vähentämisessä. Tunnistuksen oikeudenmukaisuuden parantamiseksi on tärkeää monimuotoistaa tunnistuksen kehittämiseen tarkoitettuja koulutusaineistoja sekä kehittää ratkaisuja, jotka toimivat tasapuolisesti kaikille käyttäjäryhmille.

7 Yhteenveto

Insinöörityössä tarkasteltiin älypuhelinten biometrisiä tunnistusmenetelmiä, niiden toimintaperiaatteita, luotettavuutta, tietoturvahaasteita, tulevaisuuden kehityssuuntia ja eettisiä näkökulmia. Työn tavoitteena oli selvittää, kuinka hyvin nykyiset biometriset järjestelmät tukevat älypuhelinten turvallisuutta ja käyttäjäkokemusta, millaisia riskejä niihin liittyy sekä miten ne voivat kehittyä tulevaisuudessa.

Työssä esiteltiin kolme tunnetuinta ja älypuhelimissa yleisesti käytettyä biometrisen tunnistautumisen keinoa: sormenjälkitunnistus, kasvojentunnistus ja iiristunnistus. Menetelmien luotettavuuteen perehdyttiin yleisten arviointikriteereiden sekä FAR- ja FRR-arvojen avulla. Lisäksi tarkasteltiin erilaisia haavoittuvuuksia, kuten väärennyshyökkäyksiä ja biometristen tietojen säilytystä. Näiden perusteella havaittiin, että vaikka biometriset tunnistusmenetelmät ovat usein käyttäjille helppoja ja tehokkaita, ne eivät ole täysin suojassa väärinkäytöltä ja hyökkäyksiltä.

Erityisen huomionarvoista oli, että biometrisen tiedon suojaaminen on kriittinen osa koko järjestelmän tietoturvaa. Toisin kuin perinteisiä salasanoja, biometrisiä piirteitä ei voi helposti vaihtaa, mikä tekee niiden suojaamisesta erityisen tärkeää.

Työssä tarkasteltiin myös tulevaisuuden tunnistusmenetelmiä ja tekoälyn roolia biometrisessä tunnistautumisessa. Menetelmien kehitys avaa mahdollisuuksia entistä yksilöllisempään ja tietoturvalliseen tunnistautumiseen, mutta samalla lisää eettisten pohdinnan merkitystä.

Työn tuloksena oli kokonaisvaltainen katsaus biometriseen tunnistautumiseen älypuhelimissa. Tavoitteet saavutettiin pääosin hyvin, ja työ käsitteli laajasti eri osa-alueita, joita ei olisi välttämättä hahmotettu ilman tämänkaltaista tarkastelua. Toisaalta tutkimuslähteiden laajempi vertailu ja eri älypuhelinmallien tietoturvaan perehtyminen voisivat toimia jatkotutkimuksen kohteina. Samoin biometristen tietojen lainsäädäntöön olisi hyödyllistä perehtyä tarkemmin, jotta saataisiin tietää, missä tilanteissa lainsäädäntöä sovelletaan.

Insinöörityöprosessi tarjosi mahdollisuuden syventyä ajankohtaiseen ja merkitykselliseen aiheeseen. Prosessin aikana opittiin paljon biometrisistä teknologioista, tietoturvasta sekä eettisistä kysymyksistä, jotka vaikuttavat siihen, kuinka oikeudenmukaisesti teknologiaa voidaan hyödyntää. Työn tuloksia voidaan hyödyntää esimerkiksi älypuhelinten suunnittelussa, tietoturvakäytäntöjen kehittämisessä ja käyttäjien tietoisuuden lisäämisessä biometrisen tunnistuksen mahdollisuuksista ja riskeistä.

Lähteet

1 Biometrisen tunnistamisen tietoturvallisuus ja yksityisyyden suoja. 2005. Verkkoaineisto. Liikenne- ja viestintäministeriö. <https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78695/Julkaisuja_80_2005.pdf?sequence=1&isAllowed=y>. Luettu 16.1.2025.

2 Obaidat, Mohammad S; Traore, Issa & Woungang, Isaac. 2018. Biometric-Based Physical and Cybersecurity Systems. E-kirja. Springer Nature Switzerland AG.

3 Mayron, Liam M. 2015. Biometric Authentication on Mobile Devices. Verkkoaineisto. IEEE. <https://ieeexplore-ieee-org.ezproxy.metropolia.fi/document/7118088>. 4.6.2015. Luettu 21.1.2025.

4 Khare, Pranav; Arora, Sahil & Gupta, Sandeep. 2024. Artificial Intelligence-Based Biometric Authentication Systems for Facial Recognition and Identification. Verkkoaineisto. IEEE. <https://ieeexplore-ieee-org.ezproxy.metropolia.fi/document/10738912>. 4.11.2024. Luettu 21.1.2025.

5 Priesnitz, Jannis; Rathgeb, Christian; Buchmann, Nicolas; Busch, Christoph & Margraf, Marian. 2021. An overview of touchless 2D fingerprint recognition. Verkkoaineisto. SpringerOpen. <https://doi.org/10.1186/s13640-021-00548-4>. 24.2.2021. Luettu 16.1.2025.

6 Sett, Shruti & Gupta, Himanshu. 2024. A Biometric Security Model for The Enhancement of Data Security. Verkkoaineisto. IEEE. <https://ieeexplore-ieee-org.ezproxy.metropolia.fi/document/10522414>. 14.5.2024. Luettu 16.1.2025.

7 Kunda, Douglas & Mumbi, Chisimba. 2021. A Survey of Android Mobile Phone Authentication Schemes. Mobile Networks and Applications, Vol. 26, Iss. 6, s. 2558–2566. New York: Springer Nature B.V.

8 Face ID:n käyttöä tukevat iPhone- ja iPad-mallit. 2025. Verkkoaineisto. Apple. <https://support.apple.com/fi-fi/102854>. 14.1.2025. Luettu 25.1.2025.

9 iPhonen mallin tunnistaminen. 2025. Verkkoaineisto. Apple. <https://support.apple.com/fi-fi/108044>. 15.1.2025. Luettu 25.1.2025.

10 Meng, Weizhi; Wong, Duncan S; Furnell, Steven & Zhou, Jianying. 2014. Surveying the Development of Biometric User Authentication on Mobile Phones. Verkkoaineisto. IEEE. <https://ieeexplore-ieee-org.ezproxy.metropolia.fi/document/7000543>. 31.12.2014. Luettu 11.3.2025.

11 Jha, Amaresh; Sudhakar, P; Lokhande, Sharayu Ashish Kumar; Ishodzhanova, Galina; Venkatrao, K & Zhakupova, Aliya. 2022. Facial Recognition Impact in Smartphone Sector. Verkkoaineisto. IEEE. <https://ieeexplore-ieee-org.ezproxy.metropolia.fi/document/9985766>. 29.12.2022. Luettu 23.1.2025.

12 Bowyer, Kevin W. 2011. What Suprises Do Identical Twins Have for Identity Science. Verkkoaineisto. IEEE. <https://ieeexplore-ieee-org.ezproxy.metropolia.fi/document/5958714>. 21.7.2011. Luettu 25.1.2025.

13 Kota, Jitendra Sai & Karakaya, Mahmut. 2022. Improving Off-angle Iris Recognition using Iris Quadrant Masking. Verkkoaineisto. IEEE. <https://ieeexplore-ieee-org.ezproxy.metropolia.fi/document/9764073>. 2.5.2022. Luettu 25.1.2025.

14 Thavalengal, Shejin; Bigioi, Petronel & Corcoran, Peter. 2015. Iris authentication in handheld devices – considerations for constraint-free acquisition. Verkkoaineisto. IEEE. <https://ieeexplore-ieee-org.ezproxy.metropolia.fi/document/7150600>. 8.7.2015. Luettu 25.1.2025.

15 Alrawili, Reem; AlQahtani, Ali & Khan, Muhammad. 2024. Comprehensive survey: Biometric user authentication application, evaluation, and discussion. Computers and Electrical Engineering, Vol. 119, Part A. <https://www.sciencedirect.com/science/article/pii/S0045790624004129>. 26.7.2024. Luettu 5.2.2025.

16 Iskandar, Ayman; Alfonse, Marco; Roushdy, Mohamed & El-Horbary, El-Sayed. 2024. Biometric systems for identification and verification scenarios using spatial footsteps components. Neural Computing and Applications, Vol. 36, s. 3817–3836. <https://doi.org/10.1007/s00521-023-09390-3>. 31.1.2024. Luettu 5.2.2025.

17 Arpita, Sarkar & Singh, Binod. 2020. A review on performance, security and various biometric template protection schemes for biometric authentication systems. Multimedia Tools and Applications, Vol. 79, Iss. 37–38, s. 27 721–27 776. <https://doi-org.ezproxy.metropolia.fi/10.1007/s11042-020-09197-7>. 2020. Luettu 5.2.2025.

18 Andreasson, Ari; Oravala, Juha & Toivonen, Marianne. 2023. Tietosuoja ja yksityisyys: opas jokaiselle. Helsinki: Tietosanoma.

19 Guilbon, Joffery. 2018. Introduction to Trusted Execution Environment: ARM's TrustZone. Verkkoaineisto. Quarkslab's blog. <https://blog.quarkslab.com/introduction-to-trusted-execution-environment-arms-trustzone.html>. 19.6.2018. Luettu 6.2.2025.

20 Face ID:n ja Touch ID:n suojaus. 2021. Verkkoaineisto. Apple. <https://support.apple.com/fi-fi/guide/security/sec067eb0c9e/1/web/1>. 18.2.2021. Luettu 5.2.2025.

21 Tietoja Touch ID:n edistyksellisestä suojausteknologiasta. 2024. Verkkoaineisto. Apple. <https://support.apple.com/fi-fi/105095>. 24.12.2024. Luettu 5.2.2025.

22 Biometric Authentication. 2024. Verkkoaineisto. Samsung Knox Documentation. <https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/user-authentication/biometric-authentication/>. 20.2.2024. Luettu 5.2.2025.

23 Knox Vault. 2024. Verkkoaineisto. Samsung Knox Documentation. <https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/core-platform-security/knox-vault/>. 20.2.2024. Luettu 5.2.2025.

24 Protect your privacy by heart with out privacy-protection-based design. Verkkoaineisto. Honor. <https://www.honor.com/global/privacy/features/> Luettu 5.2.2025.

25 Personal Data Processing Information. 2023. Verkkoaineisto. Huawei Developers. <https://developer.huawei.com/consumer/en/doc/Security-Guides/personal-data-0000001050990073>. 22.2.2023. Luettu 5.2.2025.

26 Ghouzali, Sanaa; Lafkih, Maryam; Abdul, Wadood; Mikram, Mounia; El Haziti, Mohammed & Aboutajdine, Driss. 2016. Trace Attack against Biometric Mobile Applications. Mobile Information Systems. <https://doi.org/10.1155/2016/2065948>. 11.4.2016. Luettu 17.2.2025.

27 Zafar, Muhammad Rehman & Shah, Munam Ali. 2016. Fingerprint authentication and security risks in smart devices. Verkkoaineisto. IEEE. <https://ieeexplore-ieee-org.ezproxy.metropolia.fi/document/7604977>. 24.10.2016. Luettu 26.2.2025.

28 Blanco Gonzalo, R; Corsetti, B; Goicoechea-Telleria, I; Husseis, A; Liu-Jimenez, J & Sanchez-Reillo, R. 2018. Attacking a Smartphone Biometric Fingerprint System: A Novice's Approach. Verkkoaineisto. IEEE. <https://ieeexplore-ieee-org.ezproxy.metropolia.fi/document/8585726>. 23.12.2018. Luettu 10.2.2025.

29 Tabassi, Elham; Chugh, Tarang; Deb, Debayan & Jain, Anil K. 2019. Altered Fingerprints: Detection and Localization. Verkkoaineisto. IEEE. <https://doi.org/10.1109/BTAS.2018.8698549>. 25.4.2019. Luettu 17.2.2025.

30 Wen, Di; Han, Hu & Jain, Anil K. 2015. Face Spoof Detection With Image Distortion Analysis. Verkkoaineisto. IEEE. <https://doi-org.ezproxy.metropolia.fi/10.1109/TIFS.2015.2400395>. 4.2.2025. Luettu 18.2.2025.

31 Akhtar, Khurram. 2024. A Guide To Liveness Detection: Enhancing Facial Recognition Security. Verkkoaineisto. Forbes. <https://www.forbes.com/councils/forbesbusinesscouncil/2024/02/09/a-guide-to-liveness-detection-enhancing-facial-recognition-security/>. 9.2.2024. Luettu 23.2.2025.

32 Zheng, Zheng; Wang, Qian & Wang, Cong. 2023. Spoofing Attacks and Anti-Spoofing Methods for Face Authentication Over Smartphones. Verkkoaineisto. IEEE. <https://ieeexplore.ieee.org/document/10061627>. 7.3.2023. Luettu 18.2.2025.

33 Smartphones have face recognition that can be easily spoofed with 2D photo, Which? finds. 2023. Verkkoaineisto. Which?. <https://www.which.co.uk/policy-and-insight/article/smartphones-have-face-recognition-that-can-be-easily-spoofed-with-2d-photo-which-finds-arM1G1p8R6mY>. 19.5.2023. Luettu 23.2.2025.

34 Brewster, Thomas. 2018. We Broke Into A Bunch Of Android Phones With A 3D-Printed Head. Verkkoaineisto. Forbes. <https://www.forbes.com/sites/thomasbrewster/2018/12/13/we-broke-into-a-bunch-of-android-phones-with-a-3d-printed-head/>. 13.12.2018. Luettu 20.2.2025.

35 Vijaykumar, Rahul; Purnapatra, Sandip; Plesh, Richard; Imtiaz, Masudul; Hou, Daqing & Schuckers, Stephanie. 2024. Deppfake Attacks on Biometric Recognition: Evaluation of Resistance to Injection Attacks. Verkkoaineisto. IEEE. <https://doi.org/10.1109/UEMCON62879.2024.10754732>. 20.11.2024. Luettu 23.2.2025.

36 Zhang, Rui & Zheng, Yan. 2018. A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification. Verkkoaineisto. IEEE. <https://ieeexplore.ieee.org/document/8590812>. 27.12.2018. Luettu 23.2.2025.

37 Smith, Daniel F; Wiliem, Arnold & Lovell, Brian C. 2015. Face Recognition on Consumer Devices: Reflections on Replay Attacks. Verkkoaineisto. IEEE. <https://doi.org/10.1109/TIFS.2015.2398819>. 3.2.2015. Luettu 23.2.2025.

38 Jain, Rubal & Kant, Chander. 2015. Attacks on Biometric Systems: An Overview. Verkkoaineisto. ResearchGate. <https://www.researchgate.net/publication/322225967_Attacks_on_Biometric_Systems_An_Overview>. Luettu 26.2.2025.

39 Sriman, Jindam; Thapar, Puneet; Alyas, Arsalan Ahmed & Singh, Urvashi. 2024. Unlocking Security: A Comprehensive Exploration of Biometric Authentication Techniques. Verkkoaineisto. IEEE. <https://doi.org/10.1109/Confluence60223.2024.10463322>. 21.3.2024. Luettu 11.3.2025.

40 Papaioannou, Maria; Mantas, Georgios; Panaousis, Emmanouil Manos; Essop, Aliyah; Rodriguez, Jonathan & Sucasas, Victor. 2023. Behavioral Biometrics for Mobile User Authentication: Benefits and Limitations. Verkkoaineisto. IEEE. <https://doi.org/10.23919/IFIPNetworking57963.2023.10186419>. 24.7.2023. Luettu 10.3.2025.

41 Cagoco, Appogel; Gubat, Sayyedatel & Asakil, Mudzna. 2023. AuthenticTap: A Behavioral Biometric Tap-Based User Authentication Method for Mobile Application. Verkkoaineisto. IEEE. <https://doi.org/10.1109/ICITISEE57756.2022.10057646>. 10.3.2023. Luettu 10.3.2025.

42 Rayani, Praveen Kumar & Changder, Suvamoy. 2023. Enhanced Unimodal Continuous Authentication Architecture on Smartphones for User Identification through Behavioral Biometrics. Verkkoaineisto. IEEE. <https://doi.org/10.1109/ViTECoN58111.2023.10157803>. 26.6.2023. Luettu 10.3.2025.

43 Karunanethy, Mukesh; Tripathi, Rahul; Panchagnula, Manesh V & Rengaswamy; Raghunathan. 2024. User authentication system based on human exhaled breath physics. Verkkoaineisto. PLOS One. <https://doi.org/10.1371/journal.pone.0301971>. 22.4.2024. Luettu 10.3.2025.

44 Srinivas, Kandala Kalyana; Vijitha, U; Chandra, G. Amruth; Kumar, K. Shiva; Peddi, Anudeep & Uppala, Bhargava Sai. 2022. Artificial Intelligence based Optimal Biometric Security System Using Palm Veins. Verkkoaineisto. IEEE. <https://doi.org/10.1109/MECON53876.2022.9752324>.14.4.2022. Luettu 11.3.2025.

45 J, Vijaya; Tiwari, Abhay; Raj, Shubham & Singh, Zorawar. 2024. Ear Pattern Based Person Recognition. Verkkoaineisto. IEEE. <https://doi.org/10.1109/WIECON-ECE60392.2023.10456501>. 26.3.2024. Luettu 12.3.2025.

46 Song, Wenwei; Kang, Wenxiong & Zhang, Yufeng. 2023. Understanding Physiological and Behavioral Characteristics Separately for High-Performance Video-Based Hand Gesture Authentication. Verkkoaineisto. IEEE. <https://doi.org/ 10.1109/TIM.2023.328725426.6.2023>. 26.6.2023. Luettu 17.3.2025.

47 Zhang, Xinman; Cheng, Dongxu; Jia, Pukun; Dai, Yixuan & Xu, Xuebin. 2020. An Efficent Android-Based Multimodal Biometric Authentication System With Face and Voice. Verkkoaineisto. IEEE. <https://doi.org/10.1109/ACCESS.2020.2999115>. 1.6.2020. Luettu 17.3.2025.

48 Huang, Long & Wang, Chen. 2024. Biometric Encoding for Replay-Resistant Smartphone User Authentication Using Handgrips. Verkkoaineisto. IEEE. <https://doi.org/10.1109/TMC.2024.3474673>. 4.10.2024. Luettu 18.3.2025.

49 Turvaa tietosi: Vinkkejä puhelimen tietoturvalliseen käyttöön. 2024. Verkkoaineisto. Kyberturvallisuuskeskus. <https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/turvaa-tietosi-vinkkeja-puhelimen-tietoturvalliseen-kayttoon>. Päivitetty 13.8.2024. Luettu 19.3.2025.

50 Näin pidät huolta tietoturvasta kotona ja työpaikalla. 2020. Verkkoaineisto. Kyberturvallisuuskeskus. <https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-pidat-huolta-tietoturvasta-kotona-ja-tyopaikalla?toggle=Salasanat&toggle=Kaksi-%20tai%20monivaiheinen%20tunnistaminen>. Päivitetty 21.7.2020. Luettu 19.3.2025.

51 Benziane, Sarah & Labed, Kaouter. 2024. Explainable AI for Biometrics. Verkkoaineisto. IEEE. <https://doi.org/10.1109/ICAMCS62774.2024.00030>. 4.12.2024. Luettu 24.3.2025.

52 Massiivinen data muuttuu mustaksi laatikoksi. 2024. Verkkoaineisto. Suomi.fi. <https://kehittajille.suomi.fi/oppaat/vastuullinen-tekoaly/maarittele-datapolitiikka/massiivinen-data-muuttuu-mustaksi-laatikoksi>. Päivitetty 7.8.2024. Luettu 24.3.2025.

53 Agrawal, Ansh; Kaur, Kirandeep & Kaur, Harkeerat. 2025. Explainable AI in Biometrics: A Novel Framework for Facial Recognition Interpretation. Verkkoaineisto. IEEE. <https://doi.org/10.1109/MoSICom63082.2024.10881703>. 18.2.2025. Luettu 25.3.2025.

54 Tekoälysäädös. 2025. Verkkoaineisto. Euroopan komissio. <https://digital-strategy.ec.europa.eu/fi/policies/regulatory-framework-ai>. Päivitetty 18.2.2025. Luettu 26.3.2025.

55 Euroopan parlamentin ja neuvoston asetus tekoälyä koskevista yhdenmukaistetuista säännöistä. 2024. Asetus 2024/1689. Verkkoaineisto. Euroopan unionin virallinen lehti. 12.7.2024. <https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:32024R1689>. Luettu 26.3.2025.

56 Erityisten henkilötietoryhmien käsittely. Verkkoaineisto. Tietosuojavaltuutetun toimisto. <https://tietosuoja.fi/erityisten-henkilotietoryhmien-kasittely>. Luettu 26.3.2025.

57 Rekisteröidyn suostumus. Verkkoaineisto. Tietosuojavaltuutetun toimisto. <https://tietosuoja.fi/rekisteroidyn-suostumus>. Luettu 26.3.2025.

58 Boogaard, Leon. 2022. User understanding and user acceptance of biometric authentication on mobile phones. Bachelor’s Thesis. Radboud University.

59 Euroopan parlamentin ja neuvoston asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta. 2016. Asetus 2016/679. Verkkoaineisto. Euroopan unionin virallinen lehti. 4.5.2016. <https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:32016R0679&qid=1743005632862>. Luettu 26.3.2025.

60 Kusyanti, Ari; Catherina, Harin Puspa Ayu; Effendrik, Popong; Santoso, Nurudin & Ekowati, Nurul Syamsi. 2024. “Risky or Trustworthy?”: User Behaviour towards Biometric Authentication Method. Procedia Computer Science, Vol. 234, s. 428–435. <https://doi.org/10.1016/j.procs.2024.03.024>. 29.4.2024. Luettu 1.4.2025.

61 Nakisa, Bahareh; Ansarizadeh, Fatemah, Oommen, Prem & Kumar, Rahul. 2023. Using and extended technology acceptance model to investigate facial authentication. Telematics and Informatics Reports, Vol. 12. <https://doi.org/10.1016/j.teler.2023.100099>. 25.9.2023. Luettu 1.4.2025.

62 Krishnan, Anoop; Neas, Brian & Rattani, Ajita. 2023. Is Facial Recognition Biased at Near-Infrared Spectrum as Well?. Verkkoaineisto. IEEE. <https://doi.org/10.1109/HST56032.2022.10025433>. 30.1.2023. Luettu 3.4.2025.

63 Albiero, Vitor; Krishnapriya, K.S.; Vangara, Kushal; Zhang, Kai; King, Michael & Bowyer, Kevin. 2020. Analysis of Gender Inequality In Face Recognition Accuracy. Verkkoaineisto. IEEE. <https://doi.org/10.1109/WACVW50321.2020.9096947>. 20.5.2020. Luettu 3.4.2025.